

**METHOD AND APPARATUS FOR SECURING ELECTRONIC GAMES**

Publication number: JP2000513983 (T)

Publication date: 2000-10-24

Inventor(s):

Applicant(s):

Classification:

- international: A63F9/24; A63F13/12; G06F19/00; H04L9/32; A63F9/24; A63F13/12; G06F19/00; H04L9/32; (IPC1-7): A63F13/12; A63F9/24; H04L9/32

- European: G07F17/32D; A63F13/12; G06F19/00B

Application number: JP19980530251T 19971219

Priority number(s): WO1997US23977 19971219; US19960775588 19961231

Also published as:

WO9829793 (A2)

WO9829793 (A3)

US6099408 (A)

US6264557 (B1)

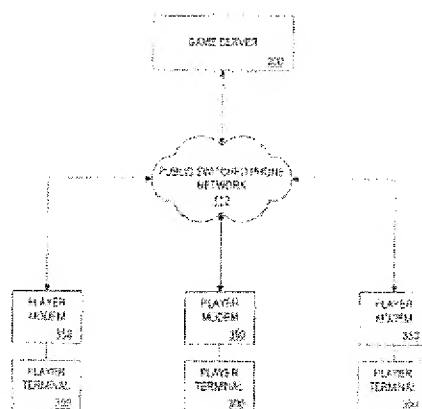
EP1021229 (A2)

more &gt;&gt;

Abstract not available for JP 2000513983 (T)

Abstract of corresponding document: **WO 9829793 (A2)**

A system for playing electronic games includes a game server (200) and one or more player terminals (300). Game results are based on a random number (225, 325) generated in each of the game server (200) and the player terminals (300). The game server (200) and the player terminals (300) cooperate to ensure that the random numbers are generated independently. As a result, game players and the game host, such as a casino, can be confident that play results are not fraudulent. In one embodiment, the random numbers (225, 325) are transmitted between the game server (200) and the player terminals (300) at substantially the same time. In other embodiments, the random numbers (225, 325) are encoded and exchanged between the game server (200) and the player terminals (300). Then, keys (294, 375) to decode the random numbers are exchanged.



Data supplied from the esp@cenet database — Worldwide

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

Prior Art Literature 1

(11) 特許出願公表番号  
特表2000-513983  
(P2000-513983A)

(43) 公表日 平成12年10月24日 (2000. 10. 24)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	特許出願 (参考)
A 6 3 F 9/24		A 6 3 F 9/24	A
H 0 4 L 9/32		13/12	M
/ A 6 3 F 13/12		H 0 4 L 9/00	C
			6 7 3 A

審査請求 有 予備審査請求 有 (全 71 頁)

(21) 出願番号 特願平10-530251  
(86) (22) 出願日 平成9年12月19日 (1997. 12. 19)  
(85) 翻訳文提出日 平成11年6月30日 (1999. 6. 30)  
(86) 国際出願番号 PCT/US 97/23977  
(87) 国際公開番号 WO 98/29793  
(87) 国際公開日 平成10年7月9日 (1998. 7. 9)  
(31) 優先権主張番号 08/775, 588  
(32) 優先日 平成8年12月31日 (1996. 12. 31)  
(33) 優先権主張国 米国 (US)

Equivalent to this literature

(71) 出願人 ウォーカー アセット マネージメント  
リミテッド パートナーシップ  
アメリカ合衆国06905 コネチカット, ス  
タンフォード, フォア ハイ リッジ パ  
ーク  
(72) 発明者 シュナイアー, ブルース  
アメリカ合衆国, ミネソタ, ミネアポリ  
ス, イー. ミネハハ, パークウェイ 101  
(72) 発明者 ウォーカー, ジェイ, エス.  
アメリカ合衆国, コネチカット, リッジフ  
ールド, スペクタクル レーン 124  
(74) 代理人 弁理士 浅村 皓 (外3名)

最終頁に続く

(54) 【発明の名称】 電子ゲームを安全保護する方法及び装置

(57) 【要約】

電子ゲームをプレーするシステムがゲーム・サーバ (200) 及び1つ以上プレーヤ端末 (300) を含む。ゲーム結果は、ゲーム・サーバ (200) 及びプレーヤ端末 (300) の各々内に発生された乱数 (225、325) に基づいている。ゲーム・サーバ (200) 及びプレーヤ端末 (300) は、乱数が独立に発生されることを保証するように適切に調整する。結果として、ゲーム・プレーヤ及び、カジノのようなゲーム・ホストは、プレー結果が不正でないことを信用することができる。1実施例では、乱数 (225、325) は、ゲーム・サーバ (200) とプレーヤ端末 (300) との間で実質的に同時に送信される。他の実施例では、乱数 (225、325) は、コード化されかつゲーム・サーバ (200) とプレーヤ端末 (300) との間で交換される。次いで、これらの乱数をデコードするキー (294、375) が交換される。

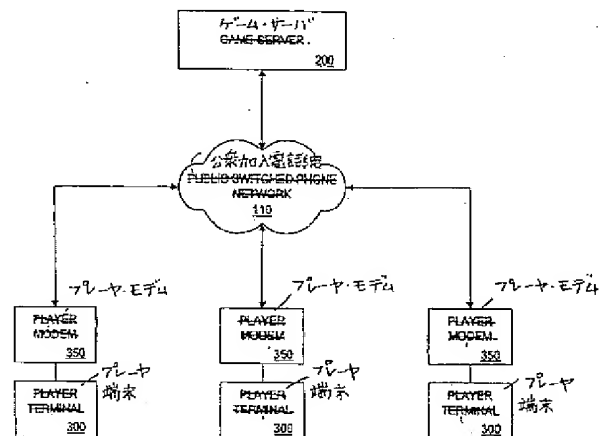


FIG. 1

## 【特許請求の範囲】

1. 電子ゲーム・システムであって、  
第1乱数を発生する第1電子システムと、  
第2乱数を発生する第2電子システムと、  
前記第1電子システムと前記第2電子システムとの間で前記第1乱数と前記第2乱数とを交換する送信機と、  
前記第1乱数が前記第2乱数と独立に発生されることを保証するプロセッサとを包含する電子ゲーム・システム。
2. 電子ゲーム・システムであって、  
ゲーム・サーバと1つ以上のプレーヤ端末とを含み、前記ゲーム・サーバが乱数発生器と、  
前記1つ以上のプレーヤ端末へ第1乱数を送信する第1送信機とを含み、  
前記1つ以上のプレーヤ端末が  
乱数発生器と、  
前記ゲーム・サーバへ第2乱数を送信する第2送信機と、  
前記第1乱数が前記第2乱数と独立に発生されることを保証するプロセッサとを含む電子ゲーム・システム。
3. 電子ゲーム・システムであって、  
ゲーム・サーバと1つ以上のプレーヤ端末とを包含し、前記1つ以上のプレーヤ端末が  
第1乱数発生器と、  
前記ゲーム・サーバへ前記第1乱数を送信する第1送信機とを含み、かつ  
前記ゲーム・サーバが  
第2乱数発生器と、  
  
前記1つ以上のプレーヤ端末へ前記第2乱数を送信する第2送信機と

を含み、かつ

前記システムが前記第1乱数と前記第2乱数とに基づいてゲーム結果を発生するプロセッサを包含する電子ゲーム・システム。

4. 請求項3記載の電子ゲーム・システムにおいて、前記1つ以上のプレーヤ端末が前記第1乱数をコード化するエンコーダを更に含み、かつ

前記ゲーム・サーバが前記コード化された第1乱数をデコードするデコーダを更に含む電子ゲーム・システム。

5. 請求項3記載の電子ゲーム・システムにおいて、前記ゲーム・サーバが前記第2乱数をコード化するエンコーダを更に含む電子ゲーム・システム。

6. 請求項5記載の電子ゲーム・システムにおいて、前記1つ以上のプレーヤ端末が

前記コード化された第2乱数をデコードするデコーダを更に含む電子ゲーム・システム。

7. 請求項3記載の電子ゲーム・システムにおいて、前記第1送信機と前記第2送信機とが実質的に同時に前記第1乱数と前記第2乱数とを送信するプロセッサを含む電子ゲーム・システム。

8. 請求項6記載の電子ゲーム・システムであって、前記第1乱数と前記第2乱数とをデコードするために前記ゲーム・サーバと前記プレーヤ端末との間でデコーディング・キーを交換する送信機を更に包含する電子ゲーム・システム。

9. 請求項4記載の電子ゲーム・システムにおいて、前記プレーヤ端末がデコーディング・キーを発生するプロセッサと、

前記ゲーム・サーバから前記第2乱数を受信する前に前記ゲーム・サーバへ前記コード化された第1乱数を送信しかつ前記ゲーム・サーバから前記第2乱数を受信した後に前記ゲーム・サーバへ前記デコーディング・キーを送信する送信機とを更に含む電子ゲーム・システム。

10. 請求項5記載の電子ゲーム・システムにおいて、前記ゲーム・サーバが

デコーディング・キーを発生するデコーダと、

前記プレーヤ端末から前記第 1 乱数を受信する前に前記プレーヤ端末へ前記コード化された第 2 乱数を送信しかつ前記プレーヤ端末から前記第 1 乱数を受信した後に前記プレーヤ端末へ前記デコーディング・キーを送信する送信機とを更に含む電子ゲーム・システム。

1 1. 請求項 3 記載の電子ゲーム・システムにおいて、前記プレーヤ端末が前記第 1 乱数のハッシュ値を発生するプロセッサと、

前記ゲーム・サーバから前記第 2 乱数を受信する前に前記ゲーム・サーバへ前記ハッシュ値を送信する送信機と、

前記ゲーム・サーバから前記第 2 乱数を受信した後に前記ゲーム・サーバへ前記第 1 乱数を送信する送信機と

を更に含む電子ゲーム・システム。

1 2. 請求項 3 記載の電子ゲーム・システムにおいて、前記ゲーム・サーバが

前記第 2 乱数のハッシュ値を発生するプロセッサと、

前記プレーヤ端末から前記第 1 乱数を受信する前に前記プレーヤ端末へ前記ハッシュ値を送信する送信機と、

前記プレーヤ端末から前記第 1 乱数を受信した後に前記プレーヤ端末へ前記第 2 乱数を送信する送信機と

を更に含む電子ゲーム・システム。

1 3. 請求項 3 記載の電子ゲーム・システムであって、

第 1 暗号化キーを使用して前記第 1 乱数又は他のプレーヤ選択データを暗号化する前記プレーヤ端末におけるエンコーダと、

前記第 1 暗号化キーに対応する少なくとも 1 つの復号キーを記憶する前記ゲーム・サーバにおけるデータベースと、

前記少なくとも 1 つの復号キーを使用して前記第 1 乱数又は前記他のプレーヤ選択データを復号する前記ゲーム・サーバにおける復号器と

を更に包含する電子ゲーム・システム。

14. 請求項3記載の電子ゲーム・システムであって、  
秘密暗号化キーを使用して前記第1乱数又は他のプレーヤ選択データを暗号化する前記プレーヤ端末における暗号化器と、

公開復号キーを使用して前記第1乱数又は前記他のプレーヤ選択データを復号する前記ゲーム・サーバにおける復号器と  
を更に包含する電子ゲーム・システム。

15. 電子ゲーム・システム用ゲーム・サーバであって、  
第1乱数を発生するプロセッサと、  
別個装置において発生された第2乱数を受信する受信機と、  
前記第1乱数と前記第2乱数とに基づいてゲーム結果を発生するプロセッサと  
、  
前記第1乱数と前記第2乱数とが独立に発生されることを保証するプロセッサと  
を含むゲーム・サーバ。

16. 電子ゲーム・システム用プレーヤ端末であって、  
第1乱数を発生するプロセッサと、  
別個装置へ前記第1乱数を送信する送信機と、  
前記第1乱数と前記別個装置で発生された前記第2乱数とに基づくゲーム結果を受信する受信機と、  
前記第1乱数と前記第2乱数とが独立に発生されることを保証するプロセッサと  
を含むプレーヤ端末。

17. 第1電子システムと第2電子システムとを含むシステム内でプレーされる電子ゲームを制御する方法であって、  
前記第1電子システムにおいて第1乱数を発生するステップと、  
第2電子システムにおいて第2乱数を発生するステップと、  
前記第1電子システムと前記第2電子システムとの間で前記第1乱数と前記第2乱数とを交換するステップと、

前記第1乱数と前記第2乱数とが独立に発生されることを保証するステップとを含む方法。

18. ゲーム・サーバと1つ以上のプレーヤ端末とを含むシステム内でプレーされる電子ゲームを制御する方法であって、

前記ゲーム・サーバにおいて第1乱数を発生するステップと、

前記プレーヤ端末において第2乱数を発生するステップと、

前記ゲーム・サーバにおいて前記第1乱数をコード化するステップと、

前記プレーヤ端末において前記第2乱数をコード化するステップと、

前記プレーヤ端末から前記ゲーム・サーバへプレーヤによってコード化された数を送信するステップと、

前記プレーヤ端末から前記ゲーム・サーバへプレーヤ・デコーディング・キーを送信するステップと、

前記第2乱数を得るために前記ゲーム・サーバにおいて前記プレーヤによってコード化された数をデコードするステップとを含む方法。

19. ゲーム・サーバとプレーヤ端末とを含むゲーム・システム用ゲーム・サーバにおいて、

第1乱数を発生するステップと、

前記第1乱数をコード化するステップと、

前記プレーヤ端末からプレーヤによってコード化された数を受信するステップと、

前記プレーヤ端末からプレーヤ・デコーディング・キーを受信するステップと、

前記プレーヤ端末へサーバ・デコーディング・キーを送信するステップと、

第2乱数を得るために前記プレーヤによってコード化された数をデコードするステップとを含む方法。

20. 請求項20記載の電子ゲームを制御する方法であって、

前記プレーヤ端末へサーバによってコード化された数を送信するステップ

を更に含む方法。

21. ゲーム・サーバとプレーヤ端末とを含むゲーム・システム用プレーヤ端末において、

第1乱数を発生するステップと、

前記第1乱数をコード化するステップと、

前記ゲーム・サーバへ前記コード化された第1乱数を送信するステップと、

前記ゲーム・サーバへプレーヤ・デコーディング・キーを送信するステップと

、

前記第1乱数と前記ゲーム・サーバにおいて発生された第2乱数とに基づくゲーム結果を受信するステップと

を含む方法。

22. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境用ゲーム・サーバにおいて、電子ゲームを制御する方法であって、

第1乱数を発生するステップと、

前記第1乱数を記憶するステップと、

前記プレーヤ端末からコード化された第2乱数を受信するステップと、

前記プレーヤ端末からデコーディング・キーを受信するステップと、

前記デコーディング・キーを使用して前記コード化された第2乱数をデコードするステップと

を含む方法。

23. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境のプレーヤ端末において、電子ゲームを制御する方法であって、

第1乱数を発生するステップと、

前記第1乱数をコード化するステップと、

前記ゲーム・サーバへ前記コード化された第1乱数を送信するステップと、

前記ゲーム・サーバが第2乱数を発生した後前記ゲーム・サーバへデコーディング・キーを送信するステップと、

前記ゲーム・サーバから前記第1乱数と前記第2乱数とに基づくゲーム結果を受信するステップと

を含む方法。

24. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境用ゲーム・サーバにおいて、電子ゲームを制御する方法であって、

第1乱数を発生するステップと、

前記第1乱数をコード化するステップと、

前記プレーヤ端末へ前記コード化された第1乱数を送信するステップと、

前記プレーヤ端末から第2乱数を受信するステップと、

前記プレーヤ端末から前記乱数が受信された後又は受信されるのと実質的に同時に前記プレーヤ端末へデコーディング・キーを送信するステップとを含む方法。

25. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境用プレーヤ端末において、ゲーム結果を得る方法であって、

前記ゲーム・サーバからコード化された第1乱数を受信するステップと、

第2乱数を発生するステップと、

前記ゲーム・サーバへ前記第2乱数を送信するステップと、

前記ゲーム・サーバへ前記第2乱数を送信した後又は送信するのと実質的に同時に前記ゲーム・サーバからデコーディング・キーを受信するステップと、

前記ゲーム・サーバから前記第1乱数と前記第2乱数とに基づくゲーム結果を受信するステップとを含む方法。

26. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境用ゲーム・サーバにおいて、電子ゲームを制御する方法であって、

第1乱数を発生するステップと、

前記プレーヤ端末から第2乱数を受信するステップと、

前記プレーヤ端末から前記第2乱数が受信されるのと実質的に同時に前記プレーヤ端末へ前記第1乱数を送信するステップとを含む方法。

27. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境用プレーヤ

端末において、ゲーム結果を得る方法であって、

第1乱数を発生するステップと、

前記ゲーム・サーバから第2乱数を受信するステップと、

前記ゲーム・サーバから前記第2乱数を受信されるのと実質的に同時に前記ゲーム・サーバへ前記第1乱数を送信するステップと、

前記ゲーム・サーバからゲーム結果を受信するステップであって、前記ゲーム結果が前記第1乱数と前記第2乱数とに基づいている前記ゲーム結果を受信するステップと

を含む方法。

28. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境用ゲーム・サーバにおいて、電子ゲームを制御する方法であって、

第1乱数を発生するステップと、

前記第1乱数を記憶するステップと、

前記プレーヤ端末からコード化された第2乱数を受信するステップと、

データベースからプレーヤ・コード化キーを検索するステップと、

前記プレーヤ・コード化キーを使用して前記コード化された第2乱数をデコードするステップと

を含む方法。

29. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境のプレーヤ端末において、ゲーム結果を得る方法であって、

第1乱数を発生するステップと、

指定プレーヤ・コード化キーを使用して前記第1乱数をコード化するステップと、

前記ゲーム・サーバへ前記コード化された第1乱数を送信するステップと、

前記ゲーム・サーバから前記第1乱数と前記第2乱数とに基づくゲーム結果を受信するステップと

を含む方法。

30. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境用ゲーム・

サーバにおいて、電子ゲームを制御する方法であって、

第1乱数を発生するステップと、

前記第1乱数を記憶するステップと、

前記プレーヤ端末からコード化された第2乱数を受信するステップと、

データベースから公開プレーヤ・コード化キーを検索するステップと、

前記公開プレーヤ・コード化キーを使用して前記コード化された第2乱数をデコードするステップと

を含む方法。

31. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境のプレーヤ端末において、ゲーム結果を得る方法であって、

第1乱数を発生するステップと、

秘密プレーヤ・コード化キーを使用して前記第1乱数をコード化するステップと、

前記ゲーム・サーバへ前記コード化された第1乱数を送信するステップと、

前記ゲーム・サーバから前記第1乱数と前記第2乱数とに基づくゲーム結果を受信するステップと

を含む方法。

## 【発明の詳細な説明】

## 電子ゲームを安全保護する方法及び装置

## 発明の背景

本発明は、電子ゲーム、特に電子ゲーム又はオンライン・ゲームの無作為性を保護及び保証する方法及び装置に関する。

種々の形式の賭博電子ゲーム (electronic game of chance) が多年出回っている。しかしながら、これらのゲームをプレーする方法は、インターネットのような電子網上で動作するデジタル・コンピュータの使用に伴って劇的に変化しつつある。プレーヤは、いまは、遠隔のサーバ及び賭け (wager) に電子的に接続することができる。

カジノへ旅行するよりはむしろ、プレーヤは自分自身の家の気楽さの中から電子ゲーム及び賭けに接続することができる。この遠隔プレーは多くの利点を有する一方、それはいくつかの安全上の論点を起こす。例えば、カジノでトランプ・ゲーム (card game) をプレー中のとき、プレーヤはディーラがトランプ札 (card) を切りかつ配るのを観察することができかつそれゆえ成行きが無作為に発生されたことに成る程度の信用を置く。電子カジノでは、札を切るプロセスはプレーヤが見ることができない乱数発生器によって典型的にデジタル的に発生され、駆動される。プレーヤは、発生された乱数が真に無作為であるか又はカジノによってこれを利するよう選択されたかどうか知ることができない。

電子ゲームプロバイダーは、賭博 (gaming) ソフトウェアが変更されていないことをプレーヤに保証することによってゲームの正当性 (legitimacy) へのプレーヤの信用を増すように試みてきている。例えば、電子ゲームプロバイダーは、独立第三者にそのソフトウェアの監査を遂行することを認めることがある。しかしながら、これは、時間を消費しかつ高く付くプロセスである。コードの数十万行に達する複雑なソフトウェアの場合、成行きの無作為性を変更するコードの2、3行を見付けることは非常に困難である。また、独立な第三者監

査者の使用は、信頼（t r u s t）の必要を他の当事者へ移行させ、ゲームの正当性を保証しない。

或る電子宝くじシステムは、遠隔プレーヤ端末と中央コントローラとの間の通信を安全保護する方法に則って（s u b s c r i b e t o）いる。例えば、コザ（K o z a）に発行された米国特許出願第4, 6 5 2, 9 9 8号は、これらの通信を安全保護する暗号方法を説明している。しかしながら、乱数の使用に依存するゲームでは、不正乱数伝送から単に保護するのでは、先行技術に固有のこれらの問題を解決しない。

ナース（K n u t h）に発行された米国特許第3, 5 4 8, 1 7 4号のような、乱数の発生を説明する多くの特許があるにもかかわらず、それらは乱数発生器の統計的性能を改善する方法を説明するにどどまる。

#### 発明の開示

したがって、本発明は、関連技術の限界及び欠点に因る1つ以上の問題を実質的に回避するようにして乱数の無作為性を保証しかつ電子ゲームの結果を認証するシステム及び方法を目指している。本発明は、ゲーム結果を発生するために使用された乱数が真に無作為な、独立に発生された数であることを保証するハードウェア及び手順を電子ゲーム・システムに含むことによって上に挙げた限界及び欠点を克服する。

先行技術の欠点を克服するために、かつ本発明に従って、具体化されかつ広く説明されるように、本発明は、ゲーム・サーバ及び1つ以上のプレーヤ端末を有する電子ゲーム・システムを含む。ゲーム・サーバは、乱数発生器及び第1乱数を1つ以上のプレーヤ端末へ送信する第1送信装置を含む。1つ以上のプレーヤ端末は、乱数発生器及び第2乱数をゲーム・サーバへ送信する第2送信装置を含む。このシステムはまた、第1乱数が第2乱数から独立に発生されることを保証するハードウェア及び手順を含む。

また、本発明の目的に従って、具体化されかつ広く説明されるように、本発明は、ゲーム・サーバ及び1つ以上のプレーヤ端末を含むシステム内でプレーされるゲームを制御する方法を述べる。この方法は、ゲーム・サーバで第1ランダム

暗号を発生するステップ、プレーヤ端末で第2乱数を発生するステップ、ゲーム・サーバで第1乱数をコード化するステップ、プレーヤ端末で第2乱数をコード化するステップ、プレーヤ端末からゲーム・サーバへプレーヤによってコード化された数を送信するステップ、プレーヤ端末からゲーム・サーバへプレーヤ・デコーディング・キーを送信するステップ、及び第2乱数を得るためにゲーム・サーバでプレーヤによってコード化された数をデコードするステップを含む。

本発明のシステム及び方法の両方について、本発明は、第1乱数及び第2乱数に基づいて結果値を発生しかつ結果値に基づいてゲーム結果を生じる。

本発明は、更に、別個にゲーム・サーバのシステムと手順及びプレーヤ端末のシステムと手順を含み、かつ第1乱数及び第2乱数をコード化し、ハッシュし、暗号化し、デコードし、デハッシュし、かつ復号するハードウェア及び手順を含む。なおまた、本発明のこれらのシステム及び手順は、プレーヤを認証することを講じ及びゲーム・データの監査記録を作成する。

上に説明されたように、或る当事者による乱数の発生に依存していた賭博のような先行技術活動では、数の真の無作為性及び数に依存する成行きの正当性に関して論点を追放することができなかった。本発明では、少なくとも2つの当事者が乱数の発生に一緒に参加しなければならず、それによっていかなる疑いも追放しかつその数の無作為性及びその数に依存するいかなる成行きをも保証する。

本発明の追加の目的及び利点が次の説明に一部は記載され、及びこの説明から一部分は明らかになり、又は本発明の実施によって学び取られると云える。本発明の目的及び利点は、添付の請求の範囲に特に指摘された素子及び組合わせによって実現されかつ達成される。云うまでもなく、上述の全般説明及び次の詳細な説明は模範的及び説明用であるに過ぎず、請求の範囲のように本発明の限定ではない。

#### 図面の簡単な説明

この明細書に組み入れられかつその部分を構成する添付図面は、本発明のいくつかの実施例を示しかつ上に与えられた全般説明及び下に与えられた詳細な説明と一緒に、本発明の原理を説明する役をする。

図1は本発明の1実施例に従う電子ゲーム・システムのブロック図である。

図2はゲーム・サーバの1実施例を示すブロック図である。

図2A及び2Bは模範的データベース構成を示すブロック図である。

図3はプレーヤ端末の1実施例を示すブロック図である。

図4はプレーヤがゲーム・サーバへ選択を送信するプロセスを示す流れ図である。

図5はプレーヤが乱数を発生しかつコード化するプロセスを示す流れ図である。

図6はゲーム・サーバが乱数を発生しかつコード化するプロセスを示す流れ図である。

図7はプレーヤ端末とゲーム・サーバとの間でデコーディング・キーを交換するプロセスを示す流れ図である。

図8は第1乱数と第2乱数の組合わせに基づいてゲーム結果を発生するプロセスを示す流れ図である。

図9はゲーム・サーバで乱数を発生しかつそれをコード化することなく送信するプロセスを示す流れ図である。

図10はプレーヤ端末からゲーム・サーバへデコーディング・キーを送信しかつ乱数をデコードするプロセスを示す流れ図である。

図11から13は乱数を交換する模範的手順を説明する流れ図であって、この手順でプレーヤ端末が乱数のハッシュ値を発生する

図14はプレーヤ端末とゲーム・サーバとの間で乱数を同時に交換する模範的手順を示す流れ図である。

図15は対称キーを使用してプレーヤ通信をコード化及びデコードする模範的手順を示す流れ図である。

図16は非対称キーを使用してプレーヤ通信をコード化及びデコードする模範的手順を示す流れ図である。

図17は認証及びメッセージ完全性を与える模範的手順を示す流れ図である。

図18は認証及びメッセージ完全性を与える他の模範的手順を示す流れ図である。

## 発明を実施するモード

## システム・アーキテクチャ

図1は、本発明の1実施例の基本的システム構成要素を示す。一般に、このシステムは、ゲーム・サーバ200及び多数のプレーヤ端末300を含み、これらのプレーヤ端末の各々が関連したプレーヤ・モデム350を伴う。ゲーム・サーバ200は、好適には、公衆加入電話網(Public Switched Telephone Network (“PSTN”))110を使用してインターネット接続を経由してプレーヤ端末モデム350に接続される。これに代えて、接続は、専用データ線路、セルラ、パーソナル通信システム(Personal Communication Systems (“PCS”))、マイクロ波網、衛星網、又はデータ通信経路のどれか他の形式によって与えられることがある。

図2は、本発明の1実施例に従うゲーム・サーバ200の基本的ハードウェア構造及びデータ構造を示す。ゲーム・サーバ200は、中央プロセッサ(“CPU”)205、暗号プロセッサ210、ランダム・アクセス・メモリ(“RAM”)215、読取り専用メモリ(“ROM”)220、乱数発生器225、支払いプロセッサ230、クロック235、オペレーティング・システム240(典型的に、ソフトウェアとしてメモリに在駐する)、網インタフェース245、及びデータ記憶装置250を含む。これらの素子は、それらの間の通信をできるように、例えば、標準システム・バスによって適当に接続される。

ゲーム・サーバ200は、好適には、かなりの数の数学計算を遂行し、かつ通信及びデータベース探索を処理する高ボリューム・トランザクション処理の能力を有する。1実施例では、ゲーム・サーバ200は、開示された機能性を遂行するために十分なメモリ及び処理能力を備えた在来のパーソナル・コンピュータ又はコンピュータ・ワークステーションを含む。普通、インテル社(Intel Inc.)によって製造された100MHz P54CのようなPentiumマイクロプロセッサがCPU205に使用されてよい。このプロセッサは、32ビット・アーキテクチャを採用する。他の実施例では、ゲーム・サーバ200は、プレーヤ端末300へ通信を送信し及びこれから通信を受信するウェブ(Web

b) サーバとして動作する。

暗号プロセッサ210は、プレーヤとの通信のコード化及びデコーディングばかりでなく、プレーヤの認証を支援する。普通、モトローラ社(Motrol a Inc.)によって製造されたMC68HC16マイクロコントローラが暗号プロセッサ210に使用されてよい。このマイクロコントローラは、16MHz構成内で16ビット乗算かつ累積命令を利用し、及び512ビット秘密キー動作を遂行するために1秒未満しか必要としない。他の模範的な商業的に出回っている暗号プロセッサには、VLSI Technologyの33MHz 6868又はSemaphore Communicationsの40MHz Roadrunner 284がある。これに代えて、暗号プロセッサ210がCPU205の部分として構成されてよい。

在来の乱数発生プロセッサが乱数発生器225に使用されてよい。例えば、富士通によって製造されたHEMT集積回路は、毎秒10億を超える乱数を発生する能力を有する。これに代えて、乱数発生器225がCPU205内へ組み入れられてよい。

支払いプロセッサ230は、支払い、課金(charge)、又は借方記入(debit)の転送又は交換を支援する。支払いプロセッサ230によって遂行される機能は、オンライン計算書、注文取り(order-taking)、クレジット・カード支払い認可、クレジット・カード清算、自動化売上げ税計算、デジタル受領書発行、勘定ベース購入追跡(account-based purchase tracking)、及び低価格サービスについての支払い総額を用意することを含む。支払いプロセッサ230によるクレジット・カード・トランザクションの処理を、Open Market社によって製造されたSecure Webserverのような商業的に出回っているソフトウェアで以て支援することもできる。このサーバ・ソフトウェアは、カード検証及び処理をハンドルするOpen Market指令部に設置されたサーバヘインターネットを通じてクレジット・カード番号を電子的に送信する。それらの統合化商業サービス(Integrated Commerce Service)はウェブ

・ベース (Web-based) 事務を実行するために必要な内勤 (back-office) サービスを提供する。支払いプロセッサ230は、好適には (インテルのPentiumのような) マイクロプロセッサを含むが、しかし、これに代えて、CPU205の部分として構成されてよい。

データ記憶装置250は、ハードディスク、磁気記憶ユニット又は光記憶ユニットばかりでなくCD-ROMドライブ又はフラッシュ・メモリを含むことがある。データ記憶装置250は、本発明におけるトランザクションの処理に使用されるデータベースを含み、これらのデータベースにはプレーヤ・データベース255、プレーヤ選択データ・データベース260、ゲーム結果データベース265、プレーヤ乱数データベース270、プレーヤ・デコーディング・キー・データベース275、監査データベース280、支払いデータベース285、プレーヤ勘定データベース290、ゲーム・サーバ乱数データベース292、ゲーム・サーバコード化キー・データベース294、ゲーム・サーバデコーディング・キー・データベース296、及び組合わせプロトコル・データベース298がある。好適実施例では、これらのデータベースを作成しかつ管理するために、Oracle社によって製造されたOracle7のようなデータベース・ソフトウェアが使用される。

解説目的のために、図2Aは模範的プレーヤ選択データ・データベース260の構造線図を与える。図示されたように、選択データ・データベース260は、プレーヤによって行われた選択に基づいてデータを維持し、かつプレーヤID番号261、追跡番号262、選択されたゲーム263、賭けの金額264、賭けの時刻266、賭けの型式267、及びゲーム結果268用フィールドを含む。

図2Bは、データベースの他の例、今度は、ゲーム結果データベース265を示す。図示されたように、ゲーム結果データベース265は、プレーヤ選択データの各集合と関連した結果を追跡しかつプレーヤID番号261、選択データ追跡番号262、ゲーム結果268、結果値269、結果の時刻271、及び支払い状況272用フィールドを含む。

これらの種々のフィールド内の情報の意味は、次の説明でいっそう明らかにな

る。他のデータベースは、類似の方法で組織され、それゆえ、各々のフィールドについて別個の図面は必要でない。プレーヤ・データベース255は、プレーヤに関するデータを維持し、名前、宛先、クレジット・カード番号、電話番号、ID番号、社会保証番号、電子メール宛先、過去システム利用、公開／秘密キー情報、及びゲーム選好（game preference）のようなフィールドを含む。この情報は、好適には、プレーヤが最初にシステムに登録するときに得られる。プレーヤ・データベース255はまた、各プレーヤ選択データの追跡番号及びプレーヤによって発生されたプレーヤ乱数を含む。

プレーヤ乱数データベース270は、全てのプレーヤ乱数を記憶する。このデータベースは、プレーヤIDによって索引付けされ、かつプレーヤID番号、対応する選択データ追跡番号、対応するプレーヤ・デコーディング・キーの追跡番号、プレーヤ乱数、及びプレーヤ乱数がゲーム・サーバ200によって受信された時刻のようなフィールドを含む。

プレーヤ・デコーディング・キー・データベース275は、プレーヤ乱数のデコーディングを容易にし、プレーヤからの通信をデコードするために必要なキーを記憶する。RSAのような公開キー暗号システムを使用して暗号化されたメッセージについては、Data Security社のプレーヤ公開キーがプレーヤ・デコーディング・キー・データベース275に記憶されることになる。データ暗号化システム（Data Encryption System（“DES”））のような対称キー暗号システムでは、対称キーが記憶される。対称キー及び公開キーの両方は、2進数字の長いストリングであり、かつ暗号認証実施例に関して下に更に十分に説明する。

監査データベース280は、プレーヤに関するトランザクション情報を記憶し、かつ、1実施例では、各プレーヤ・ログ・イン（log in）の時刻及び日付、及びプレーヤされたゲームの数を含む。

支払いデータベース285は、プレーヤによって行われた全ての支払いをプレーヤ名前、プレーヤID番号、支払いの金額、及び対応するプレーヤ選択データ及びゲーム結果のようなフィールドを用いて追跡する。このデータベースは、プ

レーヤのクレジット・カード番号又は銀行勘定情報をまた記憶することがある。

もしプレーヤが将来のトランザクションのためにゲーム・サーバ200において資金の勘定尻 (balance) を維持するように欲するならば、プレーヤ勘定データベース290が確立される。プレーヤ勘定データベース290は、当座預金 (checking account) として作用し、賭けに勝てば預金されかつ負ければ減額される。これに代えて、この勘定をプレーヤの銀行に記憶された勘定データに対するポインタであることがあり、銀行名及びプレーヤの銀行勘定番号のみを記憶する。

ゲーム・サーバ乱数データベース292は、ゲーム・サーバ200によって発生された全てのゲーム・サーバ乱数を追跡し、かつ、1実施例では、対応するプレーヤ選択データ追跡番号、プレーヤ名前、プレーヤID番号、ゲーム・サーバ乱数が発生された時刻、及びゲーム・サーバ乱数がプレーヤへ送信された時刻のようなフィールドを含む。

ゲーム・サーバ・コード化キー・データベース294は、ゲーム・サーバ乱数をコード化するためにゲーム・サーバ200によって使用される全てのコード化キーを記憶する。

ゲーム・サーバ・デコーディング・キー・データベース296は、ゲーム・サーバ乱数をデコードするためにプレーヤ端末300へ送信される全てのデコーディング・キーを記憶する。

最後に、組合わせプロトコル・データベース298は、結果値を形成するためにプレーヤ乱数をゲーム・サーバ乱数と組み合わせるために使用されるプロトコルを記憶する。

図2を再び参照すると、網インタフェース245は、それぞれのプレーヤ端末300を通してプレーヤと通信するゲートウェイである。在来の内部又は外部モデムが網インタフェース245としての役をしてよい。網インタフェース245は、好適には、1200以上のボーレートの範囲でモデムを支援するが、しかしいっそう広い帯域幅が必要とされるならば、このような入力をT1又はT3線路内へ組み合わせる。好適実施例では、網インタフェース245は、インターネッ

ト及び／又はAmerican Online、compuserve、又はProdigyのような商用オンライン・サービスに接続され、プレーヤに電子接続の広い範囲からゲーム・サーバ200にアクセスできるようにさせる。いくつかの商用電子メール・サーバが上の機能を含む。例えば、NCD Softwareは、企業網又はインターネットを通じて人々と情報をリンクするように設計された安全サーバ・ベース電子メール・ソフトウェア・パッケージ「Post Office」を製造している。この製品は、プラットフォーム非依存性でありかつインターネット・プロトコルに基づいて開放規格(open standard)を利用する。ユーザは、ファイル、グラフィック、ビデオ、及びオーディオのようなエンクロージャを用いてメッセージを交換することができる。この製品はまた、多数の言語を支援する。これに代えて、網インタフェース245は、音声メール・インタフェース、ウェブ・サイト、電子掲示板システム(electronic Bulletin Board System(“BBS”))、又は電子メール宛先として構成されることがある。

上の実施例はゲーム・サーバ200として作用する単一コンピュータを説明しているが、当業者は、機能性を複数のコンピュータにわたって分布させ、そこではデータベース及びプロセッサが別個のユニット又は位置に収容されることを実現するであろう。或るいくつかのコントローラは、一次処理機能を逐行し、かつ最少のRAM、ROMを含み、及び一般プロセッサを含む。これらのコントローラの各々は、他のコントローラ及び端末との一次通信リンクとしての役をするWANハブに取り付けられる。WANハブは、それ自体は最少処理能力しか有さなくてよく、通信ルータとしての主として役をする。当業者が納得するように、ほとんど無制限の数のコントローラが支援されると云ってよい。

図3は、本発明の好適実施例に従うプレーヤ端末の基本的ハードウェア及びデータ構造を示す。プレーヤ端末300は、好適には、中央プロセッサ(CPU)305、暗号プロセッサ310、RAM315、ROM320、乱数発生器325、ビデオドライバ327、ビデオ・モニタ330、クロック335、通信ポート340、入力装置345、モデム350、及びデータ記憶装置360を含む。

暗号認証実施例に関して下に説明されるように、バイオメトリック装置355が安全性を増すために追加されることがある。上に説明された100MHz P54CのようなPentiumマイクロプロセッサがCPU305に使用されてよい。上に説明されたHEMT集積回路のような在来の乱数発生プロセッサが乱数発生器325に使用されてよい。これに代えて、乱数発生器325がCPU305に組み入れられてよい。クロック335は、プレーヤ端末300とゲーム・サーバ200との間のトランザクションをタイム・スタンプする役をすることができる。

模範的实施例では、プレーヤ端末300は、キーボード、マウス、在来の音声認識ソフトウェア・パッケージのような入力装置を有する在来のパーソナル・コンピュータである。それゆえ、プレーヤ端末300は、モデム350を経由してゲーム・サーバ200とインタフェースすることになる。これに代えて、プレーヤ端末300は、音声メール・システム、又は他の電子又は音声通信システムであることがある。ファックス機械又はページャのような装置もまた適当な端末装置である。

もしほとんどのプレーヤ選択データ及びプレーヤ乱数がテキスト・ベース(text based)でありかつ余り長くないならば、モデム350は高速データ転送を必要としなくてよい。暗号プロセッサ310については、上に説明されたMC68HC16マイクロコントローラが使用されてよい。バイオメトリック装置355の構造は、暗号認証実施例に関連して説明する。

データ記憶装置360は、好適には、Conner Peripheralsによって製造されたもののような在来の磁気ベース・ハード・ディスク記憶ユニットを含む。選択データ・データベース365は、プレーヤによって発生された全ての選択データを記録し、選択されたゲーム、賭けの型式、賭けの金額等を追跡する。監査データベース370は、プレーヤ端末300とゲーム・サーバ200との間の通信を記憶する。コード化キー・データベース375は、ゲーム・サーバ200へ送信された通信をコード化するプロセスに使用されるキーを記憶する。組合わせプロトコル・データベース380は、プレーヤ乱数とゲーム・サーバ乱数を組み合わせるためにゲーム・サーバ200によって使用されるプロトコ

ルを記憶する。ゲーム結果データベース385は、勝ち負け金額を含む、プレーヤ結果の全てを記憶する。プレーヤ乱数データベース390は、プレーヤによって発生された各乱数を記憶する。ゲーム・サーバ乱数データベース395は、ゲーム・サーバ200から受信された全てのゲーム・サーバ乱数を記憶する。このデータベースは、ゲーム・サーバ乱数がコード化される場合に、対応するデコーディング・キーをまた記憶する。

プレーヤ端末300通信は、好適には、ソフトウェア駆動される。プレーヤ端末300によって要求された通信を使用可能とすることができる多くの商用ソフトウェア応用があり、その主要機能性はメッセージ作成及びその伝送である。例えば、Qualcomm社によって製造されたEudora Proは、メッセージの作成用編集ツールばかりでなくメッセージを適当な電子宛先へ経路選択して回送する通信ツールを供給する。ゲーム・サーバ200がウェブ・サーバとして構成されているとき、Netscape社から出されているNetscape Navigator Webブラウザのような在来の通信ソフトウェアもまた使用されてよい。プレーヤは、乱数及び選択を送信し及び受信するためにNetscape Navigator Webブラウザを使用してよい。

システム及び構成要素アーキテクチャを説明したので、電子ゲームの完全性を保証する本発明の種々の実施例を考察する。

#### 相互コード化実施例

論じられたように、本発明の1実施例では、プレーヤ端末300とゲーム・サーバ200との間の通信は、ウェブ・サーバとして作用するゲーム・サーバ200を用いて、電子網を経由して行われる。

図4は、プレーヤがプレーヤ選択をゲーム・サーバへ送信するプロセスを示す。初期的に、ステップ400で、プレーヤは、プレーヤ端末300のプレーヤ・モデム350を使用してゲーム・サーバ200にログ・オンして、通信リンクを確立する。ステップ410で、プレーヤは、可能なゲームのリストから選択することによって彼がプレーすることを欲するゲームを選択する。プレーヤは、例えば、適当なアイコン又はグラフィックをクリックすることによってウェブ・ページ上

でリストから潜在ゲームを選択する。ゲームは、好適には、ブラックジャック、クラップ、ルーレット、バカラ、スロット・マシン、宝くじ、ポーカー、ビデオ・ポーカー、スポーツ賭けを含むが、しかしプレーヤによって信頼されなければならない乱数をサーバが発生するどんなゲームを含んでもよく、これらには福引き及び賞金引き当ても入る。

ゲームが選択された後、ステップ420でプレーヤは賭けの型式を選択する。賭けの型式は、選択されたゲームに直接関係する。ルーレット・ゲームについての賭けの型式は、例えば、「偶数の」に賭けかつ「18ブラック」のような単数賭けである。ブラックジャックのようなゲームについては、プレーヤがプレーしようとする同時持ち札の数を表示することになる。

ステップ430で、プレーヤは、各賭けの金額を選択する。例えば、プレーヤは次のブラックジャック持ち札に100ドルを賭けることもあり、又はスロット・マシンの次の引きに5ドルを賭けることもある。プレーヤは、プレーヤ勘定データベースから資金を使用するように選択してもよく又は賭けた総額と一緒にクレジット・カード番号のような情報を送信してもよい。ステップ440で、プレーヤは、彼の名前又は一意プレーヤID番号を彼の選択に付加して、ゲーム・サーバ200にプレーヤの識別性(identity)を認証できるようにする。このID番号は、好適には、プレーヤがゲーム・サーバ200のサービスに登録するときゲーム・サーバから受信されるか又はプレーヤによって選択されかつ次いで電話でゲーム・サーバ200に登録される。図2Aに示されたように、ゲーム・サーバ200は、プレーヤ・データベース255にプレーヤID番号を維持しかつ一意番号のみを発行する(又は許す)。もし安全性が余り必要とされないならば、プレーヤ電話番号をID番号として役立たせることもでき、それは電話番号が一意であり及び容易に思い出せると云う両方の利点を有するからである。しかし追加の安全性が必要とされるならば、暗号認証実施例に関して下に説明されるもののような手順が実施される。

ステップ450で、プレーヤによって与えられたデータの全てが組み合わせられて「選択データ」を形成し、これがゲーム・サーバ200へ送信される。それ

で、ゲーム・サーバ200は、プレーヤ選択データを受信し、かつそれを選択データ・データベース260に記憶する前に追跡番号を付加する。

World Wide Webベース・インタフェースの代わりに、プレーヤは、電子メール、音声メール、又はファクシミリ伝送を経由して選択データを送信してもまたよい。音声メールを用いる場合、プレーヤはゲーム・サーバ200を呼び出しかつ選択データをオーディオ形式で残す。次いで、選択データは、ゲーム・サーバ200で、図示されていない在来オーディオ・テキスト・トランスライバによってデジタル・テキストに転記される。説明されたように、ゲーム・サーバ200は、複数の伝送方法を支援し、選択データの広範な多様な形式を扱うことを配慮する。

図5は、プレーヤがゲーム・サーバ200によって使用される乱数を発生しかつコード化するプロセスを示す。ステップ500で、プレーヤは、自身で数を選択することによって又は乱数を生じるようにプレーヤ端末300の乱数発生器225をプロンプトすることによってのどちらかでプレーヤ乱数を発生する。この数は好適には無作為であるにもかかわらず、このシステムはゲーム・サーバ200によって予測され得ないどんな数に関しても等しく働く。乱数発生器225は、プレーヤのキー入力(key stroke)間の時間、又はコンピュータ・マウス345の現在位置のような外部ファクタを組み込むことがある。ステップ510で、プレーヤ端末300は、プレーヤ乱数をプレーヤ乱数データベース390に記憶する。ステップ520で、暗号プロセッサ310がコード化キー・データベース375からのコード化キーを使用してプレーヤ乱数をコード化する。各プレーヤ乱数は、好適には、一意コード化キーを使用すると云う理由から、コード化キー・データベース375は、好適には、多数の一意キーを含むか又は実時間に新コード化キーを発生するかのどちらかである。数をコード化する種々の方法は、技術上知られており、したがって、ここに詳細に説明する必要はない。参考に、当業者は、ブルース・シュナイアー、応用暗号技術、プロトコル、アルゴリズム及びC言語でのソース・コード(第2版、ジョン・ウィリー・アンド・ソーンズ社、1996年)(Bruce Schneier, Applied Cryptography)

ptography, Protocols, Algorithms, And Source Code In C, (2rd Ed, John Wiley & Sons, Inc., 1996))を参照してもよい。

プレーヤが乱数をどの賭けに適用するかゲーム・サーバ200が知るように、プレーヤは、コード化されたプレーヤ乱数と一緒に、彼のプレーヤID番号及び対応する選択データに対する追跡番号(図2A参照)を付加する。次いで、ステップ530で、この情報がプレーヤ・モデム350を使用してゲーム・サーバ200へ送信される。プレーヤの識別性を認証するために、ゲーム・サーバ200は、コード化されたプレーヤ乱数を含むメッセージからプレーヤID番号を抽出しかつプレーヤ・データベース255内のプレーヤ識別性を捜し出す。もし更なる認証が望まれるならば、下に論じられる認証実施例のプロトコルが採用される。

図6は、ゲーム・サーバ乱数を発生しかつコード化するためにゲーム・サーバ200によって使用される手順を示す。プレーヤを認証した後、ステップ600で、ゲーム・サーバ200の乱数発生器225がゲーム・サーバ乱数を発生する。ステップ610で、ゲーム・サーバ乱数がゲーム・サーバ乱数データベース292に記憶される。ステップ620で、ゲーム・サーバ200の暗号プロセッサ210がゲーム・サーバ乱数をコード化する。プレーヤ乱数のコード化の場合のように、暗号プロセッサ210は、好適には、一意コード化キーの大きな補給又はそれらを生じるアルゴリズムを有する。次いで、ステップ630で、ゲーム・サーバ200は、コード化されたゲーム・サーバ乱数プレーヤ端末300へ送信する。注意すべきであるのは、プレーヤ端末300でのコード化されたゲーム・サーバ乱数の受信についてのいくつかのハードウェア・オプションがあることである。

この実施例では、乱数が発生されておりかつ将来の検証のために交換されているが、しかしまだデコードされていないと云う理由で、システムが安全に保たれる。それとして、両当事者は、それらの乱数が独立に発生されており、公正なゲーム結果を保証することを知る。

図7は、プレーヤ端末300とゲーム・サーバ200との間でデコーディング

・キーを交換する手順を示す。ステップ700で、ゲーム・サーバ200が（最初に）ゲーム・サーバ・デコーディング・キーをプレーヤ端末300へ送信する。ゲーム・サーバ乱数をコード化するのに使用されたコード化キーのように、ゲーム・サーバ・デコーディング・キーは、発生された各乱数に対して一意でなければならない。ステップ710で、プレーヤ端末300が一意プレーヤ・デコーディング・キーをゲーム・サーバ200へ送信する。この実施例で、デコーディング・キーの交換は同時に行われる必要はなく、それは両当事者が各々他のコード化された乱数を既に所有しているからである。ステップ720で、ゲーム・サーバ200は、プレーヤ乱数をデコードするためにプレーヤ・デコーディング・キーを使用する。この時点で、ゲーム・サーバ200は、デコードされた形でプレーヤ乱数及びゲーム・サーバ乱数の両方を有しかつゲーム結果を発生するためにこれらの乱数を使用することができる。下に説明されるように、プレーヤは、疑いのある場合コード化されたゲーム・サーバ乱数をデコードするだけでよい。図8は、ゲーム・サーバ200がゲーム結果を発生するための手順を示す。図示されたように、ゲーム・サーバ200は、組合わせプロトコル・データベース298（図2）からの組合わせプロトコルを使用してゲーム・サーバ乱数及びデコードされたプレーヤ乱数に基づいてゲーム結果を発生する。ステップ800で、組合わせプロトコルが組合わせプロトコル・データベース298から検索される。組合わせプロトコルは、好適には、プレーヤ端末300及びゲーム・サーバ200の両方に知られており、選択された特定ゲームに一意であり、かつ読む誰に対しても発行されてよい。組合わせプロトコルは、好適には、一連の数学的ステップであって、プレーヤ乱数及びゲーム・サーバ乱数を明確に区別できる「結果値」に変換する。例えば、ルーレット・ゲームに対して開発された組合わせプロトコルは、プレーヤ乱数及びゲーム・サーバ乱数がまず互いに乗ぜられて、生じる数が平方されることを表示する。この生じた数を「38」で除した後、その剰余が「結果値」である。したがって、この例では、結果値は「0」と「37」との間の整数である。ルーレットゲームに対しては、「0」と「37」との間の整数がルーレット円盤の回転に対する「38」の可能な成行き集合で以て写像さ

れる。それゆえ、結果値は、ルーレット円盤の回転の結果に相当する。

次いで、ステップ810で、ゲーム結果を決定するために、結果値がデータベース260内のプレーヤ選択データ内の賭けの型式と比較される。例えば、ルーレットの例では、「15赤」（図2A参照）に賭けるプレーヤは、もしも結果値が「15赤」以外のどれかの数であったならば、賭けに負けるだろう。負けのゲーム結果は、1ドル賭けたならば「1ドルを失なう」ことになる。次いで、ステップ820で、ゲーム結果がプレーヤ端末300へ送信される。次いで、ゲーム・サーバ200の支払いプロセッサ230がプレーヤ勘定290を1ドルだけ減額するか、又はプレーヤのクレジット・カードに1ドル課金し（ステップ830）、次いでゲーム結果を、プレーヤID番号によって索引付けされたゲーム結果データベース265に記憶する（ステップ840）。改善された監査形跡（*audit trail*）のために、1実施例では、ゲーム結果が記憶される前に、これがゲーム・サーバ200のクロック235によってタイムスタンプされるか、又は先に記憶されたゲーム結果に暗号的に連鎖させられる。次いで、選択データ・データベース260に記憶された対応するプレーヤ選択データが、ステップ850で或る1つの結果に到達したことを表示するために更新される（例えば、図2の「結果」欄参照）。プレーヤは、そこで、プレーヤ選択データの他の集合を選択することによってサイクルを再び開始する。

上の方法を使用して、プレーヤは、乱数が互いに独立に発生されたこと、すなわち、プレーヤ乱数がゲーム・サーバ乱数の知識なしで発生された、又はこの逆に発生されたことを信頼することができる。ゲーム・サーバ200がだますには、ゲーム・サーバは、ゲーム・サーバ乱数を発生する前にプレーヤ乱数をデコードしなければならないことになる。プレーヤ乱数の知識があれば、ゲーム・サーバ200は、所望結果値、それゆえ、ゲーム結果を得るためにゲーム・サーバ乱数を選択することもできる。しかしながら、ゲーム・サーバ乱数を発生する前にプレーヤ乱数を得ることは、ゲーム・サーバ200がコード化されたプレーヤ乱数をデコードすることを必要とし、これはプレーヤ・デコーディング・キーを受信する前に実際に完遂することができない。もしゲーム・サーバ200がプレーヤ乱

数を適正に組み入れないことによってだましたとプレーヤが疑うならば、プレーヤは、ゲーム・サーバ・デコーディング・キーを使用してゲーム・サーバ乱数をデコードすることができかつプレーヤ端末300の組合わせプロトコル・データベース398からの組合わせプロトコルを両乱数に適用し、それゆえゲーム結果を検証することができる。

#### 単一コード化実施例

本発明の他の実施例では、プレーヤ端末300とゲーム・サーバ200がやはり乱数を交換する。しかしながら、この実施例は、当事者のうちの一方のみがその乱数をコード化することを必要とする。コード化することなくその乱数を送信する当事者は、好適には、自分が他の当事者からコード化された乱数を受信するまで待機する。この実施例を図9及び10を参照して論じる。

図9を参照すると、プレーヤ端末300が相互コード化実施例について説明したのと類似の方法で、プレーヤ乱数を既に発生し、それをコード化し、かつそれをゲーム・サーバ200へ送信してしまっている。ゲーム・サーバ200は、ステップ900でゲーム・サーバ乱数を発生し、かつステップ910でそれをゲーム・サーバ乱数データベース292に記憶する。ステップ920で、ゲーム・サーバ200は、ゲーム・サーバ乱数をプレーヤ端末300へ送信する。しかしながら、コード化が行われないから、ゲーム・サーバ200は、ゲーム・サーバ・デコーディング・キーを送信しない。

図10に示されたように、ゲーム・サーバ乱数を受信した後、ステップ1000で、プレーヤ端末300は、プレーヤデコーディング・キーをゲーム・サーバ200へ送信する。ステップ1010で、ゲーム・サーバ200は、コード化されたプレーヤ乱数をデコードするためにプレーヤ・デコーディング・キーを使用する。この時点で、各当事者は、他の当事者のそれぞれの乱数を所有している。次いで、これらの乱数が上に説明されたように組み合わせられてゲーム結果を発生する。

この実施例では、プレーヤ端末300は、ゲーム・サーバ200がゲーム・サーバ乱数を発生しかつ送信する前に、コード化されたプレーヤ乱数を発生しかつ

送信する。次いで、ゲーム・サーバ乱数を受信した後、プレーヤ端末300は、ゲーム・サーバ200がコード化されたプレーヤ乱数をデコードするためのデコーディング・キーを送信する。代替実施例では、ゲーム・サーバ200とプレーヤ端末300が手順を入れ替える。特に、ゲーム・サーバ200は、プレーヤ端末300がプレーヤ乱数を発生しかつ送信する前に、コード化されたゲーム・サーバ乱数を発生しかつ送信する。次いで、プレーヤ乱数を受信した後、ゲーム・サーバ200は、プレーヤがゲーム・サーバ乱数をデコードするために、もしもプレーヤそのように望むならば、デコーディング・キーを送信する。

やはり、これらの実施例では、プレーヤ乱数及びゲーム・サーバ乱数が独立に開発されたことをプレーヤ及びゲーム・サーバ200の両方が信用することができる。

#### ハッシュ値実施例

この実施例では、プレーヤ端末300もゲーム・サーバ200もどちらもそれぞれのそれぞれの乱数をコード化しない。代わりに、プレーヤ端末300は、プレーヤ乱数を発生し、それをハッシュし、ハッシュ値をゲーム・サーバ200へ送信し、次いで、ゲーム・サーバ乱数を受信する。次いで、プレーヤ端末は、プレーヤ乱数をゲーム・サーバ200へ送信し、ここでこの乱数がハッシュされ、次いで、この乱数がプレーヤ端末300によって元々発生された乱数であるかどうか判定するために、先に受信されたハッシュ値と比較される。この実施例の動作が図11～13が流れ図に示されている。

図11を参照すると、プレーヤ端末300は、上に説明されたように、プレーヤ選択データをゲーム・サーバ200へ既に送信してしまっている。次いで、ステップ1100で、プレーヤ端末300は、先に説明されたように、プレーヤ乱数を発生する。ステップ1110で、プレーヤ乱数がプレーヤ端末300のプレーヤ乱数データベース390に記憶される。次いで、暗号プロセッサ310がステップ1120でプレーヤ乱数をハッシュし、ハッシュ値を発生する。このハッシュ値は、元のプレーヤ乱数の一方向変換を表す。プレーヤ乱数からハッシュ値を発生することは計算上簡単であるが、ハッシュ値だけからゲーム・サーバ乱数

を再作成することは、計算上実行可能ではない。ステップ1130で、プレーヤ端末300は、ハッシュ値をゲーム・サーバ200へ送信する。

図12に示されたように、次いで、ステップ1200で、ゲーム・サーバ200は、ゲーム・サーバ乱数を発生する。この数は、プレーヤ乱数に基づくことはできない。それは、この実施例では、ゲーム・サーバ200がプレーヤ乱数のハッシュ値を処理するだけであるからである。ステップ1210で、ゲーム・サーバ200は、ゲーム・サーバ乱数をゲーム・サーバ乱数データベース292に記憶し、次いで、ステップ1220で、ゲーム・サーバ乱数をプレーヤ端末へ送信する。

図13を参照すると、ステップ1300で、プレーヤ端末300は、ゲーム・サーバ乱数を受信しかつ記憶する。次いで、ステップ1310で、プレーヤ端末300は、未ハッシュ・プレーヤ乱数をゲーム・サーバ200へ送信する。ステップ1320で、ゲーム・サーバ200の暗号プロセッサがプレーヤ乱数をハッシュし、結果のハッシュ値をプレーヤ端末300から受信したハッシュ値と比較する。もしこれらのハッシュ値が一致するならば、ゲーム・サーバ200は、プレーヤ端末300が変更プレーヤ乱数を提出しなかったことを保証される。両乱数をいまや所有しているので、ゲーム・サーバ200は、上に説明されたようにゲーム結果を発生するように進む。

単一コード化実施例の場合のように、ハッシュ値動作の1実施例では、プレーヤ端末300が上に説明されたようにその乱数のハッシュ値を発生しかつ送信する。しかしながら、代替実施例では、乱数のハッシュ値がゲーム・サーバ200によって発生されることがあり、この場合、ゲーム・サーバ200及びプレーヤ端末の対応する手順がやはり入れ替えられる。

#### 同時交換実施例

この実施例では、プレーヤ端末300及びゲーム・サーバ200が同時に乱数を交換し、乱数の発生 of 独立性を保証するためのどんなコーディング又はハッシュ動作の必要も除去する。

図14は、この実施例に対する手順を示す。図14で、プレーヤ端末300は、

上に説明されたように、プレーヤ選択データを既に送信してしまっている。ステップ1400で、プレーヤ端末300は、プレーヤ乱数を発生し、次いで、ステップ1410で、それをプレーヤ乱数データベース390に記憶する。ステップ1420で、ゲーム・サーバ200は、ゲーム・サーバ乱数を発生し、かつステップ1430でそれをゲーム・サーバ乱数データベース290に記憶する。ステップ1440で、プレーヤ乱数及びゲーム・サーバ乱数が電子掲示板へ同時に通知(p o s t)される。1実施例では、これは、それらの乱数を通知しようとする時刻を設定することによって完遂される。例えば、両当事者が乱数を午後3時に通知することに同意し、かつこの時刻をそれらのそれぞれの通信ソフトウェアに組み入れる。午後3時に通信ソフトウェア(別個に図示されていない)がそれらの乱数を自動的に通知する。だましを阻止するために、電子掲示板のオペレーティング・システムが同意通知時刻から10分の1秒以内に通知されたどの乱数も無効にすることもできる。この時間要件は、好適には、組合わせプロトコルを使用する逆計算を計算上実行不可能にするほど短い。

いったんプレーヤ乱数及びゲーム・サーバ乱数が通知されてしまうと、この実施例に対する手順は、ゲーム結果を発生するために、上に説明されたように進行する。

#### 多数プレーヤ実施例

上の実施例は、一人のプレーヤがゲーム・サーバ200と対話するプロトコルを説明している。多数のプレーヤであっても、各プレーヤを個々に取り扱うと共に、プレーヤ達が個々のゲーム結果を受信することによって、容易にハンドルすることができる。例えば、5人のルーレット・プレーヤがプレーヤ選択データを提出しかつ異なる結果値に基づいてゲーム結果を受信することができる。これに代えて、プレーヤは、彼らのプレーヤ乱数を組み合わせかつ単一商用結果値に基づいてゲーム結果を受信することもできる。このようにして、ゲーム・サーバ200は、プレーヤのグループが円盤の同じ回転に基づいて勝ち又は負けに直面する物理的カジノにいつそう良く似てくる。

先に説明された実施例におけるように、多数プレーヤ実施例では、各プレーヤ

が彼らがやりたい賭けの型式を記述する選択データを発生する。次いで、ゲーム・サーバ200がゲーム・サーバ乱数を発生しかつそれを暗号プロセッサ210を使用しでコード化する。各プレーヤ端末300がプレーヤ乱数を発生しかつそのそれぞれの暗号プロセッサ310で以てコード化する。次いで、各プレーヤ端末300は、そのコード化されたプレーヤ乱数をゲーム・サーバ200へ送信する。いったんゲーム・サーバ200が全てのコード化された乱数を収集すると、このゲーム・サーバはコード化された乱数を各プレーヤ端末300へ送信する。コード化されたゲーム・サーバ乱数を受信した後、各プレーヤ端末300は、そのプレーヤ・デコーディング・キーをゲーム・サーバ200へ送信する。ゲーム・サーバ200は、各コード化されたプレーヤ乱数をデコードしかつこれらの乱数を組合わせプロトコル・データベース298からの組合わせプロトコルを使用してゲーム結果を発生するために使用し、データベース298はゲームに許されたプレーヤの最大数までのプレーヤの種々の数に対する異なる組合わせプロトコルを記憶することができる。ゲーム結果は、各プレーヤ端末300へ送信される。プレーヤ達は、デコードされたプレーヤ乱数を互いに交換しかつそれらをゲーム・サーバ乱数と、これをゲーム・サーバ・デコーディング・キーで以てデコードした後、比較することによって、結果値を検証することができる。

他の実施例では、各プレーヤ端末300は、プレーヤ選択データ及びプレーヤ乱数を発生する。第1プレーヤが彼のプレーヤ乱数をコード化ししかつそれを第2プレーヤへ送信する。第2プレーヤは彼のプレーヤ乱数を第1プレーヤからのコード化された乱数と連結し、かつ両数を、それらを第3プレーヤへ送る前に、コード化する。このプロセスがプレーヤの各々毎に続く。最終プレーヤは、組合わせプレーヤ乱数をゲーム・サーバ200へ送る。ゲーム・サーバ200は、ゲーム・サーバ乱数を作成し、それをコード化し、次いでそれを各プレーヤへ送信する。ゲーム・サーバによってコード化された乱数を受信した後、各プレーヤ端末300は、そのプレーヤ・デコーディング・キーをゲーム・サーバ200へ送信する。ゲーム・サーバ200の暗号プロセッサ210がこれらのデコーディング・キーを使用して組合わせプレーヤ乱数をデコードし、結果値を形成し、かつ

各プレーヤに対するゲーム結果を生じる。

上に説明された相互コード化実施例の代わりに、上に説明されたものと一貫するハッシュアルゴリズム、単一コーディング、及び同時交換手順を多数プレーヤの対話を容易にするために使用してよい。

#### 単一事象対多数事象実施例

ギャンブリング・ゲームの成行きは、単一事象又は多数事象のどちらかによって決定される。ルーレット及びスロットは、単一成行きがゲーム結果を決定するので、単一事象の良い例である。ルーレット円盤の1回転がその回転に賭けられた全ての賭けを完全に解決する。スロット・マシン賭けの結果は、プレーヤが勝つ又は負けるかどうか決定するのに単一ハンドル引きを必要とする。これらの単一事象ゲームでは、ゲーム結果を決定するために結果値がプレーヤ選択データと容易に比較される。

しかしながら、多数事象ゲームでは、ゲーム結果は、多数結果値に基づいていると云える。ブラックジャックは、多数事象ゲームの1例である。プレーヤが1勝負(a hand)を勝つかどうかは、プレーヤの札とディーラの札次第である。1枚の札を表すために単一結果値を発生するのでは不充分である。代わりに、本発明の1実施例では、結果値が52枚の札の完全な一続き(sequence)を表す。いったん札の一続きがプレーヤ乱数及びゲーム・サーバ乱数に基づいて定められると、札を配ることができる。

例えば、コード化されたプレーヤ乱数を発生しかつそれをゲーム・サーバ200へ送信した後、プレーヤ端末300は、コード化されたゲーム・サーバ乱数を受信する。次いで、プレーヤ端末300はゲーム・サーバ200へデコーディング・キーを送信し、ゲーム・サーバは札の一組(deck)内の札の完全な一続きを表す結果値を発生する。プレーヤ端末300へゲーム・サーバ・デコーディング・キーを送信する前に、ゲーム・サーバ200は、結果値から発生された札の一続きから配られた持ち札を表すプレーヤ札値を送信する。もしプレーヤが望むならば、プレーヤは彼のブラックジャック持ち札に追加札を、やはり、札の決められた一続きから引くことを選択する。いったん持ち札が選択されると、ゲー

ム・サーバ200は、ゲーム・サーバ・デコーディング・キーをプレーヤ端末300へ送信する。プレーヤがこのキーを、追加札を引くようにプレーヤの選択を行う前に、受信しないことが重要である。それは、ゲーム・サーバによってコード化された乱数をデコードすることがプレーヤに札の完全な一続きを知らせることにもなるからである。

ブラックジャック・ゲームをハンドルする他の方法は、配られた各札毎に結果値を発生することである。（プレーヤ選択データを確立することによって）プレーヤの賭けを行った後、プレーヤは一連のプレーヤ乱数を発生し、持ち札に必要な各札毎に交換する。したがって、ゲーム結果は、結果値の各々が本発明の説明された手順を通して作成された、7つ又は8つの結果値を必要とすることもある。

#### 暗号認証実施例

本発明の或る種の実施例では、プレーヤ選択データ及びプレーヤ乱数の出所（authorship）の認証は、付加ID又は名前を検査しかつそれをプレーヤ・データベース255に記憶されたものと比較することを伴う。代替実施例では、暗号プロトコルが認証プロセスに追加される。これらのプロトコルは、メッセージの送信側を認証する能力を強化しかつ通信自体の完全性を検証する役をし、それが伝送中変更されていないことを証明する。暗号は、盗聴者が通信の内容を聞き知るのを防止する。このような技術は、暗号保証方法と一般に称されるべきであり、かつ対称キー及び非対称キーの両方ばかりでなくデジタル・シグネチャ及びハッシュ・アルゴリズムの使用を含む。

送信側の認証ばかりでなく通信の完全性を保証するために暗号プロトコルを使用する慣習は、技術上周知であり、ここに詳細に説明する必要はない。ブルース・シュナイアー、応用暗号技術、プロトコル、アルゴリズム及びC言語でのソース・コード（第2版、ジョン・ウィリー・アンド・ソنز社、1996年）（Bruce Schneier, Applied Cryptography, Protocols, Algorithms, And Source Code in C, (2rd Ed, John Wiley & Sons, Inc., 1

996) ) に説明されたようなどれか従来の暗号プロトコルを本発明に従って使用することもできかつ暗号プロセッサ210によって実行することになる。

図15は、プレーヤ端末300及びゲーム・サーバ200がキーを共用する対称キー実施例を示す。それゆえ、(別個に又はプレーヤ通信として一緒に称される) プレーヤ選択データ及びプレーヤ乱数の暗号化及び復号の両方が同じキーで以て遂行される。この暗号化は、DES (FIPS PUB 46に指定された米国政府標準) のようなアルゴリズムで以て、又はIDEA、Blowfish、RC4、RC2、SAFER等のような技術上知られたいくつかのアルゴリズムのうちのどれかで以て実施してよい。

初期的に、プレーヤは、プレーヤ端末300の暗号プロセッサ310を使用して、ステップ1500で、彼の指定した対称キーで以て彼の通信を暗号化する。そのキーは、コード化キー・データベース375に記憶されてよく、又は、そうでなければ、プレーヤによって記憶され又はメモリ化される。次いで、ステップ1510で、プレーヤ通信がゲーム・サーバ200の暗号プロセッサ210へ送信される。暗号プロセッサ210は、プレーヤ通信からプレーヤIDを抽出し(ステップ1520)、プレーヤ・データベース255内のプレーヤの対称キーを捜し出し(ステップ1530)、かつこのキーで以てプレーヤ通信を復号する(ステップ1540)。ゲーム・サーバ・コード化キー・データベース294は通信を暗号化する、復号する、及び/又は認証するアルゴリズム及びキーを含む。ステップ1550で、暗号プロセッサ210は、その生じる通信が了解性であるかどうか決定する。もし了解性であるならば、その通信は同じキーによって暗号化されているに違いなく、そのプレーヤがそのメッセージのまさに著者であるに違いないことを認証する。云うまでもなく、これらの暗号技術は、上に説明された適当な乱数暗号化技術に加えて、通信の安全性を保護するために採用される。

この手順は、無認可プレーヤが正当プレーヤとして自己を表すのを困難にする。暗号手順を用いないならば、正当プレーヤからサンプル通信を得た無認可プレーヤはプレーヤIDを抽出し、次いで、このID番号を無認可通信に付加することができかもしれない。しかしながら、プレーヤ通信が対称キーで以て暗号化さ

れているとき、サンプル・プレーヤ通信を得る無認可プレーヤはプレーヤのID番号を見付けるのみで、対称キーを見付けない。このキーがないと、無認可プレーヤは認可プレーヤができたと同じ方法でこのプレーヤ通信を暗号化することができないから、無認可プレーヤはゲーム・サーバ200をだますプレーヤ通信を作成することができない。通信の変更は対称キーの知識を必要とするから、対称キー・プロトコルはまた、プレーヤ通信が伝送中に変更されていないことを保証する。暗号化プレーヤ通信はまた、プレーヤにいつそうの匿名性を与える。

図16は、プレーヤ通信が秘密キーで以て暗号化されかつ公開キーで以て復号される非対称キー・プロトコルを示す。非対称キー・プロトコルに対する2つのこのようなアルゴリズムは、RSAアルゴリズム及びデジタル・シグナチュア・アルゴリズム(Digital Signature Algorithm (“DSA”))である。ステップ1600で、プレーヤ端末300が暗号プロセッサ310を使用してプレーヤの秘密キーで以てプレーヤ通信を暗号化する。次いで、ステップ1610で、プレーヤ端末300は、プレーヤ通信をゲーム・サーバ200へ送信する。次いで、ゲーム・サーバ200の暗号プロセッサ210が、ステップ1620でプレーヤIDを抽出し、ステップ1630でプレーヤ・データベース255内のそのプレーヤに関連した公開キーを捜し出し、かつステップ1640でこの公開キーで以てその通信を復号する。前のように、ステップ1650で、もしプレーヤ通信が了解性であるならば、ゲーム・サーバ200はそのプレーヤを認証している。やはり、プレーヤ通信がゲーム・サーバによって受信される前にその通信を得る無認可プレーヤはこの通信を検出されないで変更することはできないが、それは、プレーヤの秘密キーを無認可プレーヤは知らないからである。しかしながら、もしプレーヤの公開キーを無認可プレーヤがなんとかして得たとしたならば、無認可プレーヤはメッセージを読むことができるかもしれない。もしプレーヤがプレーヤ通信を彼の秘密キーで以て暗号化して、このプレーヤの通信を閲覧するにはこのプレーヤの秘密キーを知ることが無認可プレーヤに必要とさせるならば、通信の秘密は保たれる。

図17は、認証及びメッセージ完全性を与えるためにデジタル・シグナチュ

アを使用する暗号技術を示す。1つのこのようなアルゴリズムはDSAである。上に説明された非対称プロトコルにおけるように、各プレーヤが関連した公開キー及び秘密キーを有する。各プレーヤは、暗号プロセッサ310を用いてステップ1700で彼の秘密キーで以て彼の通信にサインし、ステップ1710でそれをゲーム・サーバ200へ送信する。ゲーム・サーバ200で、暗号プロセッサ210がステップ1720でプレーヤIDを抽出しかつステップ1730でプレーヤの公開キーを捜し出し、ステップ1740で通信及びプレーヤの公開キーを使用してシグナチュアを検証する。ステップ1750で、もし通信が了解性であるならば、ゲーム・サーバ200は通信を真正であるとして受理する。

図18を参照すると、プレーヤ通信の真正性及び完全性を検証するメッセージ認証コードを使用する暗号技術が示されている。本発明のハッシュ・プロトコルでは、プレーヤ端末300及びゲーム・サーバ200が対称キーを共用し、このキーをステップ1800でプレーヤが通信のハッシュに含める。ハッシュ・プロトコルでは、一方向性関数が通信のデジタル表現に適用される。RIPE-MAC、IBC-Ha s h、CBC-MAC等のようなMACアルゴリズムのうちのどれかがこの応用に適用されることがある。ステップ1810で通信をゲーム・サーバ200へ送信した後、ステップ1820でゲーム・サーバ200の暗号プロセッサ210がプレーヤ通信からプレーヤIDを抽出する。次いで、ステップ1830で暗号プロセッサ210がプレーヤの対称キーを捜し出しかつステップ1840で対称キーで以て通信をハッシュし、生じるハッシュ値を通信に付加されたハッシュ値と比較する。もしステップ1850でこれらの値が一致するならば、通信の完全性がプレーヤの真正性と一緒に検証される。

暗号技術はプレーヤ通信の真正性に大きな信頼を与えることができるにもかかわらず、もしプレーヤの暗号キーを漏出するならばこれらの技術は役に立たない。他のプレーヤの対称キーを得る無認可プレーヤはゲーム・サーバ200の眼には他のプレーヤと区別がつかない。そのプレーヤが通信の真の著者であったか又は正しい暗号キーを持つ無認可プレーヤでかどうか知るすべがない。1実施例では、指紋読取り装置、音声認識システム、レチナール (r e t i n a l) スキャナ等

のようなバイオメトリック装置355（図3）がこのこの問題を解決することを助ける。バイオメトリック装置はプレーヤの肉体的属性を通信に組み入れ、それで、この属性がゲーム・サーバ200のプレーヤ・データベース255に記憶された値と比較される。

例えば、指紋検証は、通信の作成前に、通信の発生中に、所定の又は無作為の時刻に、ゲーム・サーバ200からのプロンプトに応答して、又はプレーヤ端末300に走査レンズを組み入れかつ通信が発生されている間連続検証のためにプレーヤに指を走査レンズ上に終始維持するように要求することによって連続的に、実行される。

このようなバイオメトリック装置の例は、台湾の会社、StarTekから出回っているFC100 FINGERPRINT VERIFIERである。FC100は、インタフェース・カードを経由してどんなPCにも容易に適応可能である。この指紋検証装置は、光学走査レンズを使用する。プレーヤは指をそのレンズの上に置き、生じる画像が走査され、デジタル化され、かつそのデータが圧縮されてメモリに記憶される。典型的に、256バイトが必要とされる全てである。各生走査（live-scan）指紋がデータ記憶装置360に記憶された先に登録され／記憶されたテンプレートと比較される。もしこれらの指紋が一致しないならば、暗号プロセッサ310によって実行される暗号アルゴリズムはそのプレーヤが通信を発生するのを禁止する。

音声検証実施例では、プレーヤの音声は彼の識別性を検証するために使用される。この実施例は、標準電話接続上で実施することができるから、なんら特殊化したハードウェアの使用を必要とすることがないと云う利点を有する。プレーヤの識別性は、ゲーム・サーバ200で検証される。声紋を得かつその後それを使用して人の識別性を検証するプロセスは、技術上周知であり、したがってここで詳細に説明する必要はない。在来スピーカ識別ソフトウェアがプレーヤの音声をサンプルする。このサンプルは、ゲーム・サーバ200でプレーヤ・データベース255に記憶される。プレーヤが通信をゲーム・サーバ200へ送信しようと欲する度に、彼はゲーム・サーバ200を呼び出しかつ音声サンプルのための

プロンプトの際に電話に声を入れることを要求される。もしこのサンプルがプレーヤ・データベース255に記憶されているものと一致するならば、プレーヤはパスワードを供給され、このパスワードは彼の通信に付加されたデジタル・シグナチュアに組み入れられる。適当な音声一致パスワードを備えていないいかなる通信も受理されない。声紋も、プレーヤの通信を作成することを許すのに先立ち局域的にプレーヤの識別性を検証するために、プレーヤ端末300のデータ記憶装置360内のデータベースに記憶されることがある。

#### 匿名トランザクション実施例

先に述べたように、本発明は、プレーヤの匿名を扱うことを考慮する。このような匿名は、全ての通信についてプレーヤの名前に対する全ての参照を除去することによって完遂される。例えば、盗聴者がプレーヤの識別性を発見することを防止するには、プレーヤは、プレーヤ選択データに彼の名前でなくてむしろ彼のIDを含めることになる。プレーヤ・データベース255に記憶されたプレーヤのIDの検出を防止するためには、ID番号を、好適には、ゲーム・サーバ200の公開キーで以て暗号化する。

識別性の追加保護として、プレーヤは、インターネットに見られる在来の匿名回送者を通してゲーム・サーバ200と通信することもできる。

#### 支払い実施例

本発明は支払い特徴に関する用意なしで実施することができるが、上述のシステムの支給者が収益の流れを引き出すための多くの方法がある。1実施例では、提出されたプレーヤ選択データの集合毎に均一料金が課される。他の実施例では、所与に時間間隔にわたってプレーヤ選択データのどれかの数の集合に対して均一料金を課して、プレーヤに新聞を購読するよりは多くのサービスを購読できるようにする。他の実施例では、広告主がプレーヤに対するウェブ・ページと一緒にメッセージを掲げてもらったものに支払い、これでシステムの運営費用を補足する。

現在、本発明の好適実施例及び好適方法であると考えられるものを図示しかつ説明したが、当業者にとって云うまでもないように、本発明の真の範囲から逸脱

することなくこれらに種々の変更及び変形を行うことが可能であり、かつこれらの素子を等価素子で置換することも可能である。

更に、本発明の中心範囲から逸脱することなく多くの変形を本発明の教示に従う特定素子、技術、又は実施に適合するように行うことも可能である。したがって、この発明はここに開示した特定実施例及び方法に限定されるのではなく、本発明は添付の請求の範囲に入る全ての実施例を含むことを意図する。

【図1】

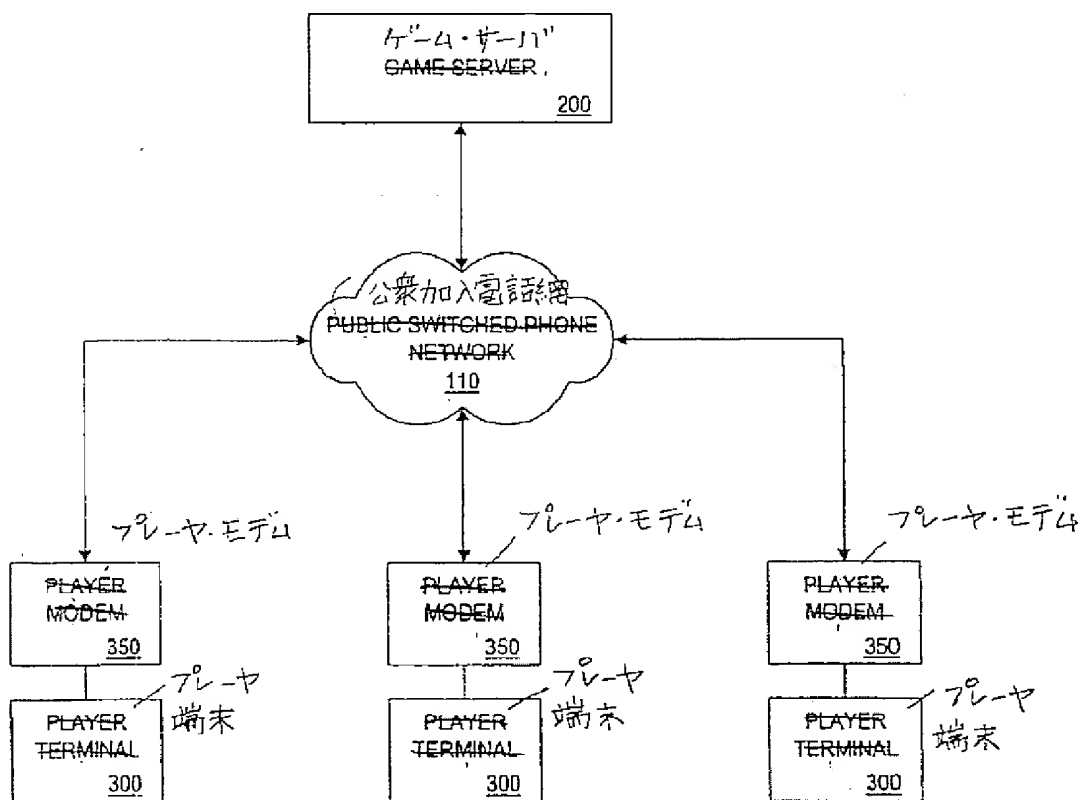


FIG. 1

【図2】

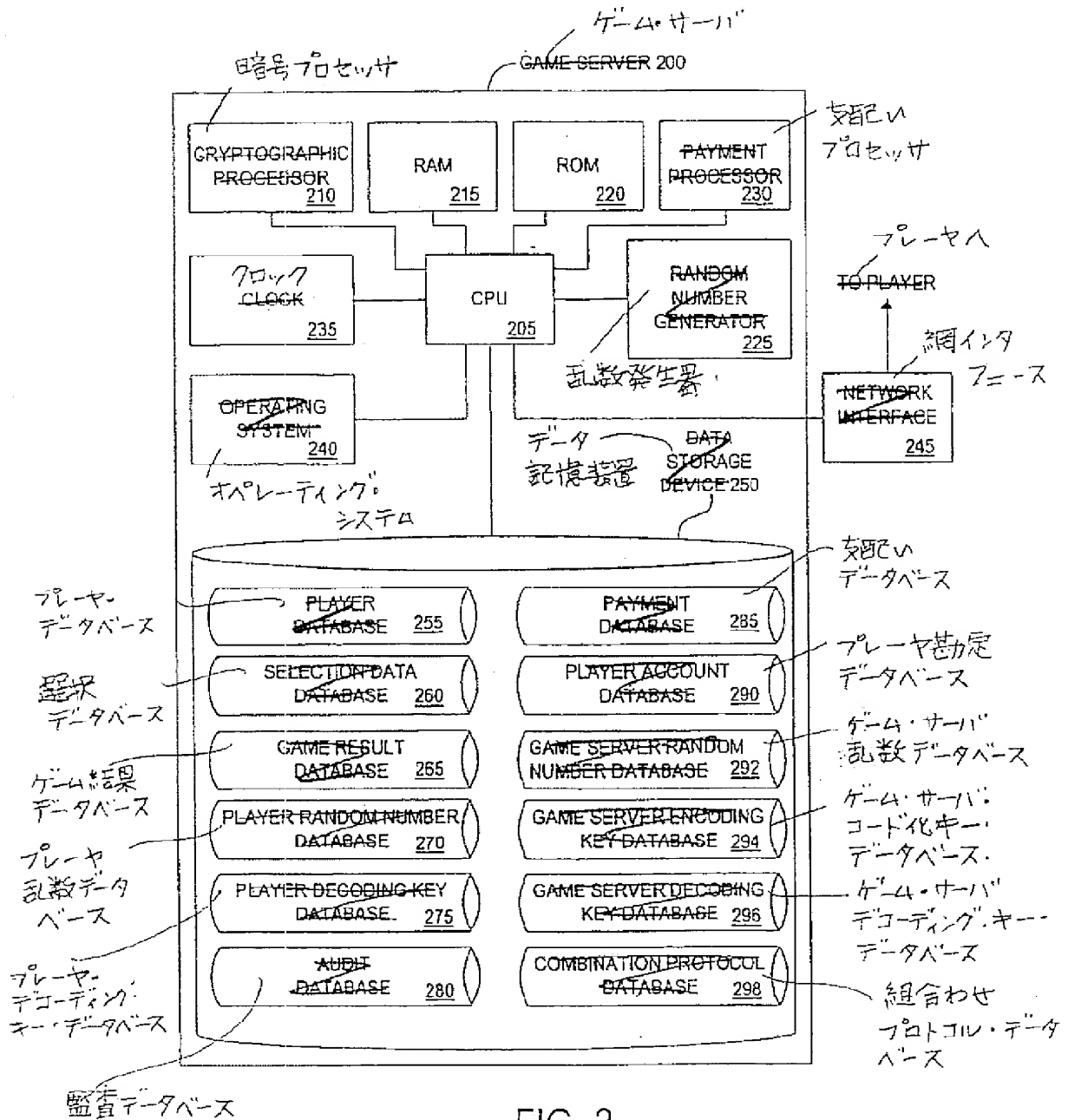


FIG. 2

【図2】

選択データデータベース  
SELECTION DATA  
DATABASE 260

プレイヤーID 番号	追跡番号	選ばれた ゲーム	賭け の金額	賭け の時刻	賭け の型式	ゲーム 結果
PLAYER ID NUMBER 261	TRACKING NUMBER 262	GAME SELECTED 263	AMOUNT OF WAGER 264	TIME OF WAGER 265	TYPE OF WAGER 267	GAME RESULT 268
GP45921	4032XF	ROULETTE ルーレット	\$5.00	5:10 PM 05/07/97	FIFTEEN RED 15 赤	WIN-勝ち \$5.00
HT21990	9724MR	BLACKJACK ブラックジャック	\$10.00	3:30 AM 05/08/97	TWO HANDS 2 持ち手	LOSE-負け \$10.00
DL44087	8322PK	BLACKJACK ブラックジャック	\$15.00	3:35 AM 05/08/97	ONE HAND 1 持ち手	WIN-勝ち \$15.00

FIG. 2A

ゲーム結果データベース  
GAME-RESULT-DATABASE 265

選手データ  
追跡番号

プレイヤーID PLAYER-ID NUMBER 261	SELECTION DATA TRACKING NUMBER 262	ゲーム結果 GAME-RESULT 268	結果値 RESULT-VALUE 269	結果の時刻 TIME-OF RESULT 271	支払い状態 PAYMENT STATUS 272
GB45921	4032XF	WIN \$5.00	34	5:15 PM 05/07/97	PAYMENT COMPLETED 支払い完了
HT21990	9724MR	LOSE \$10.00	234	3:32 AM 05/08/97	PAYMENT DUE 支払い済み
DL44087	8322PK	WIN \$15.00	876	3:37 AM 05/09/97	AMOUNT UPDATED 金額更新

FIG. 2B

【図3】

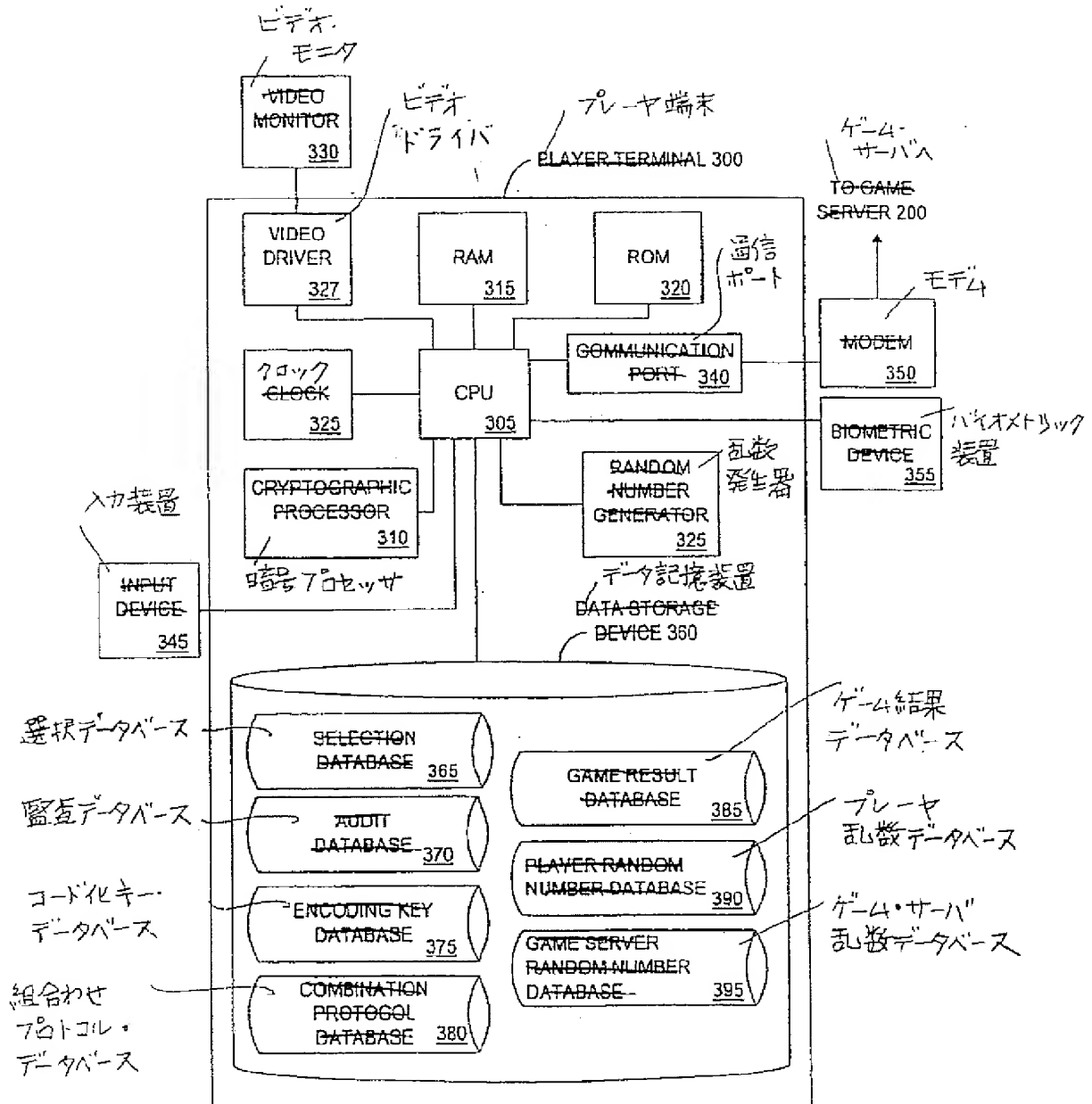


FIG. 3

【図 4】

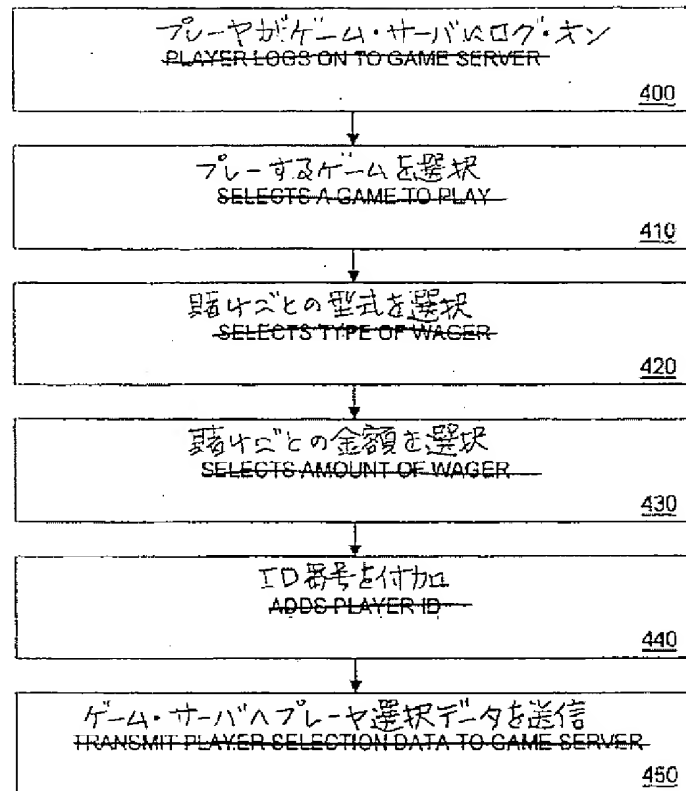


FIG. 4

【図 5】

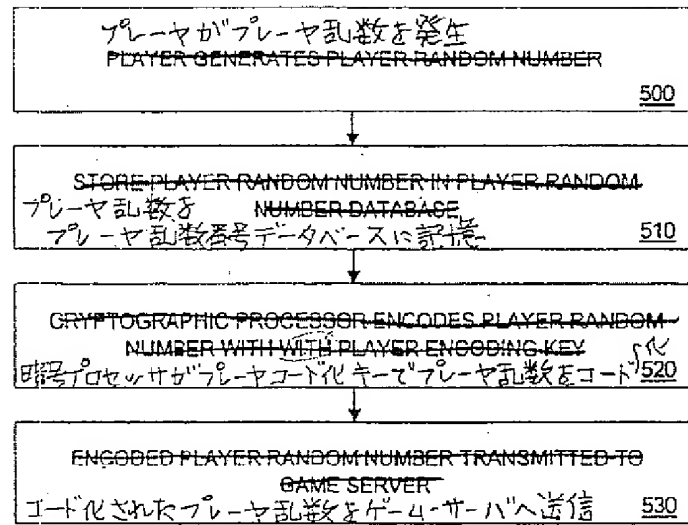


FIG. 5

【図6】

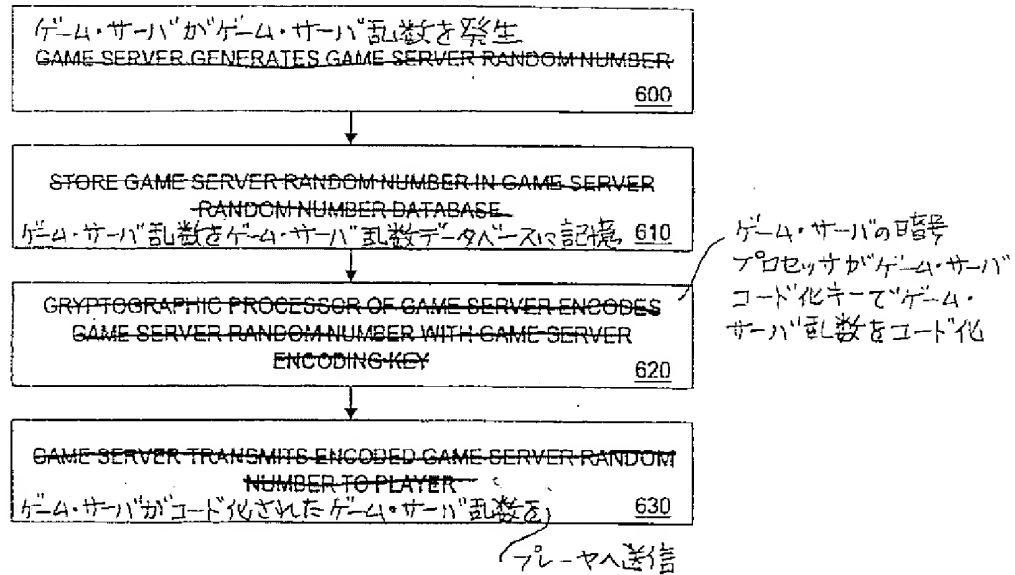
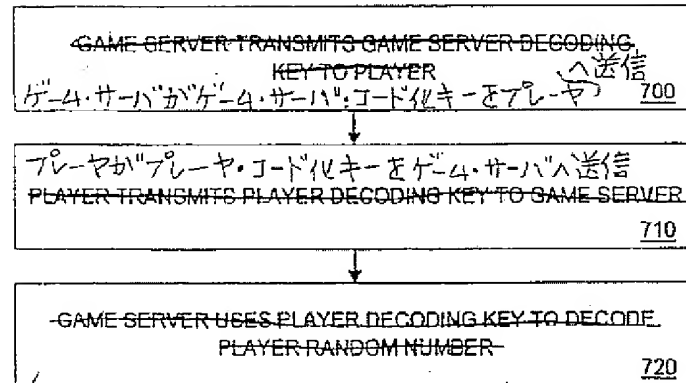


FIG. 6

【図7】



プレイヤー乱数をデコードするためゲームサーバが  
プレイヤー・デコーディング・キーを使用。

FIG. 7

【図8】

ゲームサーバが組合わせプロトコルをプレイヤー乱数とゲームサーバ  
乱数に適用することによって結果値を発生

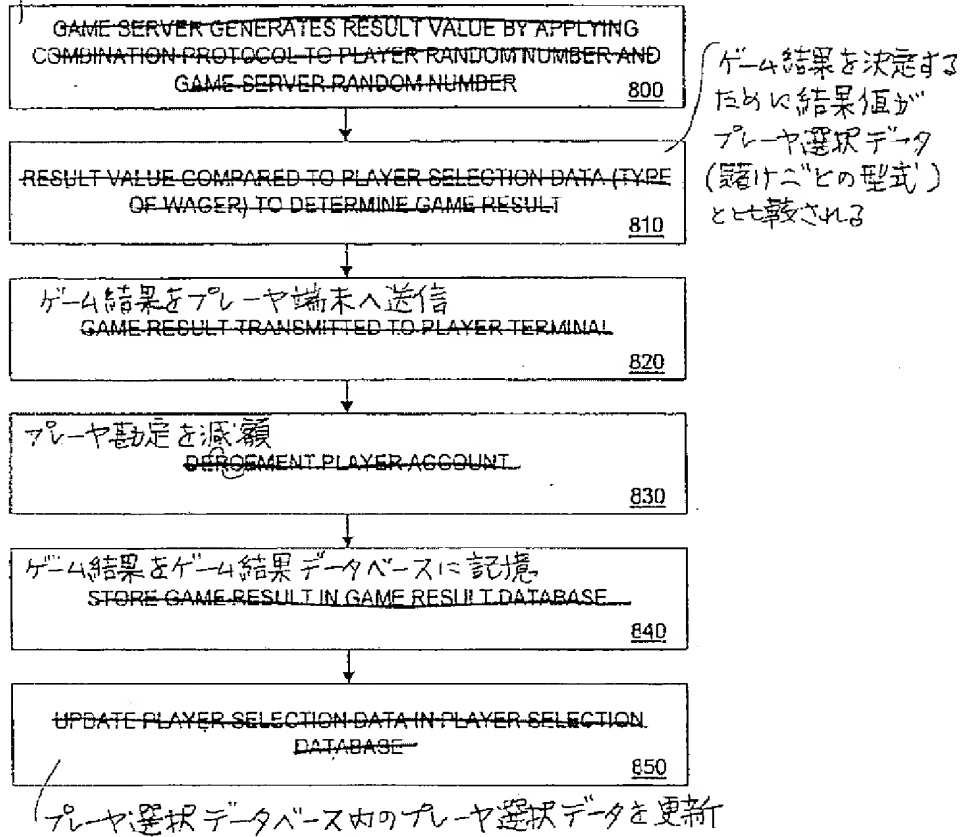


FIG. 8

【図9】

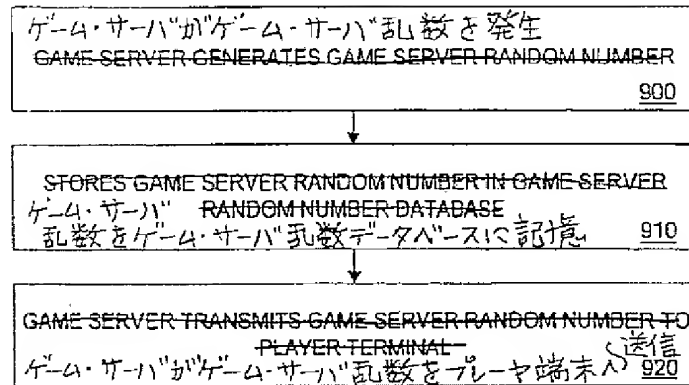


FIG. 9

【図10】

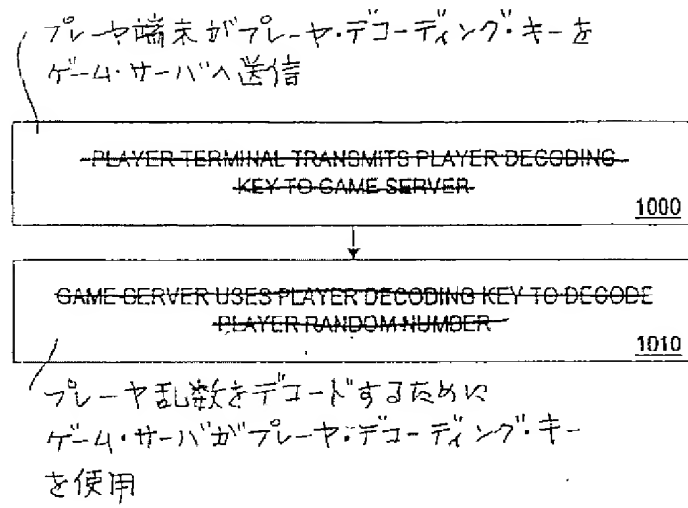


FIG. 10

【図11】

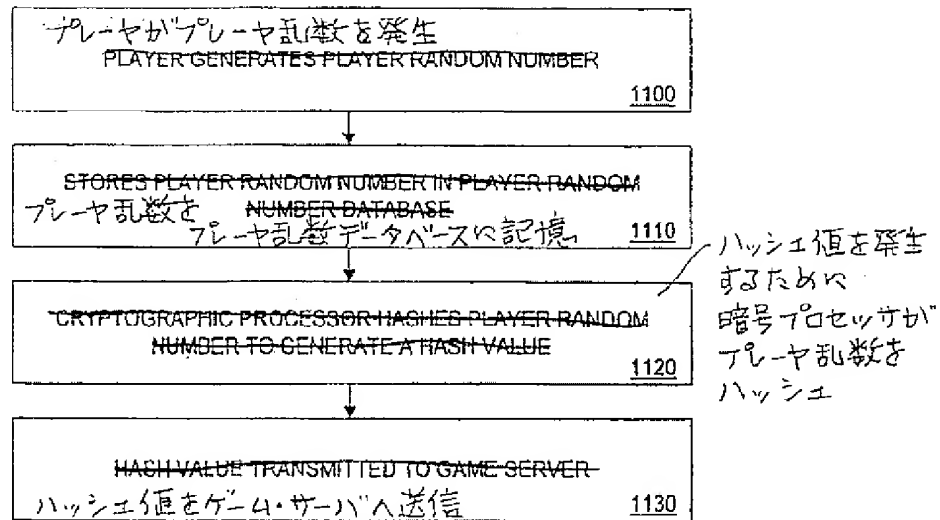


FIG. 11

【図12】

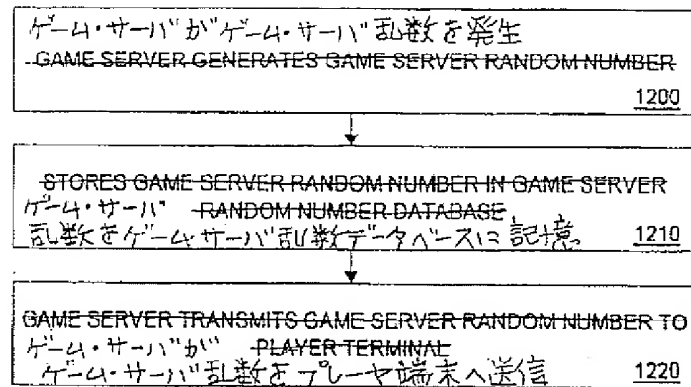


FIG. 12

【図13】

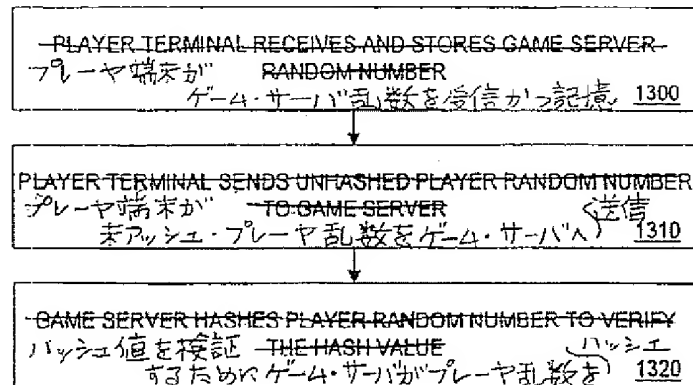


FIG. 13

【図 14】

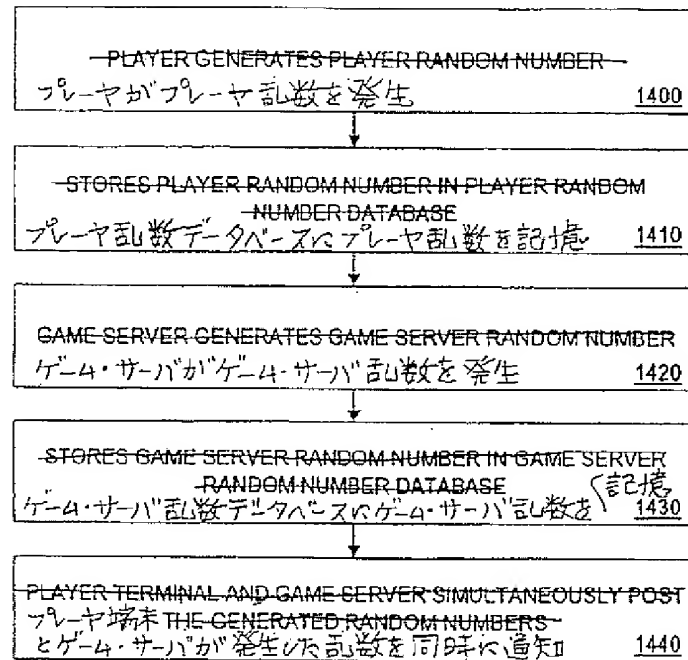


FIG. 14

【図 15】

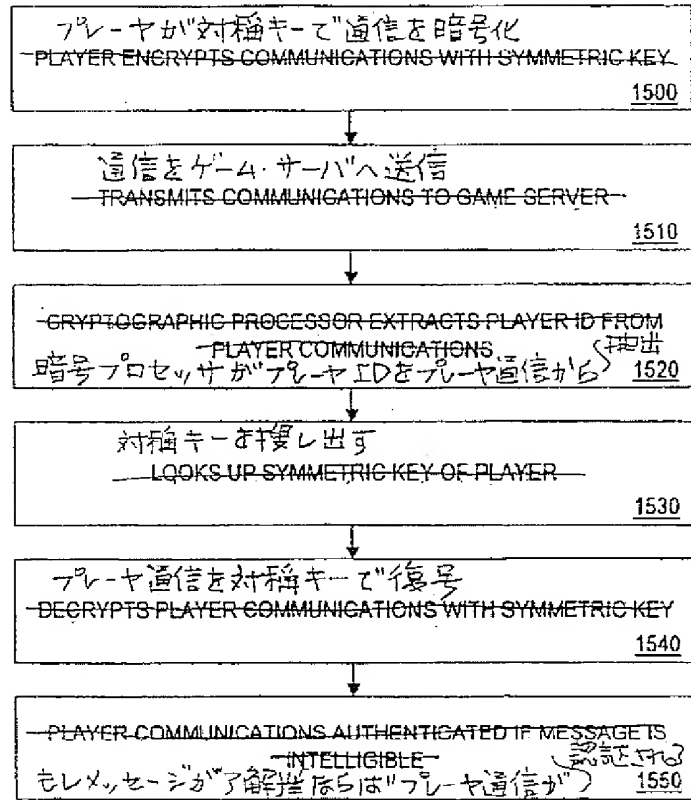


FIG. 15

【図16】

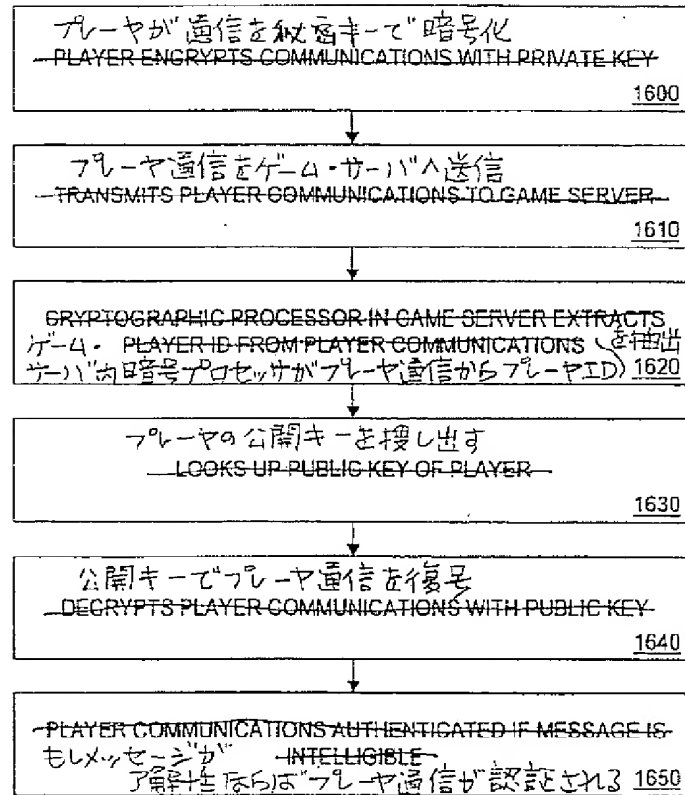


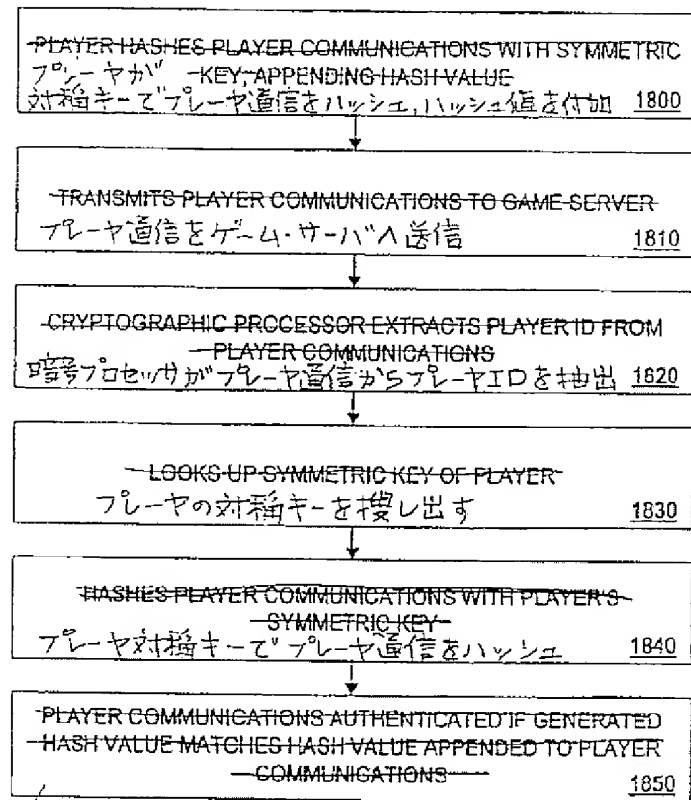
FIG. 16

【図17】



FIG. 17

【図18】



もし発生されたハッシュ値がプレイヤー通信の付加されたハッシュ値と一致すれば「プレイヤー通信が認証される

FIG. 18

## 【手続補正書】

【提出日】平成11年11月18日（1999. 11. 18）

## 【補正内容】

## 請求の範囲

1. 電子ゲーム・システムであって、  
第1乱数を発生する第1電子システムと、  
第2乱数を発生する第2電子システムと、  
前記第1電子システムと前記第2電子システムとの間で前記第1乱数と前記第2乱数とを交換する送信機と、  
前記第1乱数が前記第2乱数と独立に発生されることを保証するプロセッサとを含む電子ゲーム・システム。
2. 電子ゲーム・システムであって、  
ゲーム・サーバと1つ以上のプレーヤ端末とを含み、前記ゲーム・サーバが乱数発生器と、  
前記1つ以上のプレーヤ端末へ第1乱数を送信する第1送信機とを含み、  
前記1つ以上のプレーヤ端末が  
乱数発生器と、  
前記ゲーム・サーバへ第2乱数を送信する第2送信機と、  
前記第1乱数が前記第2乱数と独立に発生されることを保証するプロセッサとを含む電子ゲーム・システム。
3. 電子ゲーム・システムであって、  
ゲーム・サーバと1つ以上のプレーヤ端末とを包含し、前記1つ以上のプレーヤ端末が  
第1乱数発生器と、  
前記ゲーム・サーバへ前記第1乱数を送信する第1送信機とを含み、かつ  
前記ゲーム・サーバが

第2乱数発生器と、

前記1つ以上のプレーヤ端末へ前記第2乱数を送信する第2送信機と  
を含み、かつ

前記システムが前記第1乱数と前記第2乱数とに基づいてゲーム結果を発生するプロセッサを包含する電子ゲーム・システム。

4. 請求項3記載の電子ゲーム・システムにおいて、前記1つ以上のプレーヤ端末が前記第1乱数をコード化するエンコーダを更に含み、かつ

前記ゲーム・サーバが前記コード化された第1乱数をデコードするデコーダを更に含む電子ゲーム・システム。

5. 請求項3記載の電子ゲーム・システムにおいて、前記ゲーム・サーバが前記第2乱数をコード化するエンコーダを更に含む電子ゲーム・システム。

6. 請求項5記載の電子ゲーム・システムにおいて、前記1つ以上のプレーヤ端末が

前記コード化された第2乱数をデコードするデコーダ  
を更に含む電子ゲーム・システム。

7. 電子ゲーム・システムであって、

ゲーム・サーバと1つ以上のプレーヤ端末とを包含し、前記1つ以上のプレーヤ端末が

第1乱数発生器と、

前記ゲーム・サーバへ前記第1乱数を送信する第1送信機と  
を含み、かつ

前記ゲーム・サーバが

第2乱数発生器と、

前記1つ以上のプレーヤ端末へ前記第2乱数を送信する第2送信機と  
を含み、かつ

前記システムが前記第1乱数と前記第2乱数とに基づいてゲーム結果を発生するプロセッサを包含し、前記第1送信機と前記第2送信機とが実質的に同時に前記第1乱数と前記第2乱数とを送信するプロセッサを含む電子ゲーム・システム。

8. 請求項6記載の電子ゲーム・システムであって、前記第2乱数をデコードするために前記ゲーム・サーバと前記プレーヤ端末との間でデコーディング・キーを交換する送信機を更に包含する電子ゲーム・システム。

9. 請求項4記載の電子ゲーム・システムにおいて、前記プレーヤ端末が

デコーディング・キーを発生するプロセッサと、

前記ゲーム・サーバから前記第2乱数を受信する前に前記ゲーム・サーバへ前記コード化された第1乱数を送信しかつ前記ゲーム・サーバから前記第2乱数を受信した後に前記ゲーム・サーバへ前記デコーディング・キーを送信する送信機と  
を更に含む電子ゲーム・システム。

10. 請求項5記載の電子ゲーム・システムにおいて、前記ゲーム・サーバが

デコーディング・キーを発生するデコーダと、

前記プレーヤ端末から前記第1乱数を受信する前に前記プレーヤ端末へ前記コード化された第2乱数を送信しかつ前記プレーヤ端末から前記第1乱数を受信した後に前記プレーヤ端末へ前記デコーディング・キーを送信する送信機と  
を更に含む電子ゲーム・システム。

11. 請求項3記載の電子ゲーム・システムにおいて、前記プレーヤ端末が前記第1乱数のハッシュ値を発生するプロセッサと、

前記ゲーム・サーバから前記第2乱数を受信する前に前記ゲーム・サーバへ前記ハッシュ値を送信する送信機と、

前記ゲーム・サーバから前記第2乱数を受信した後に前記ゲーム・サーバへ前記第1乱数を送信する送信機と  
を更に含む電子ゲーム・システム。

12. 請求項3記載の電子ゲーム・システムにおいて、前記ゲーム・サーバが

前記第2乱数のハッシュ値を発生するプロセッサと、

前記プレーヤ端末から前記第1乱数を受信する前に前記プレーヤ端末へ前記ハ

ッシュ値を送信する送信機と、

前記プレーヤ端末から前記第1乱数を受信した後に前記プレーヤ端末へ前記第2乱数を送信する送信機と

を更に含む電子ゲーム・システム。

13. 請求項3記載の電子ゲーム・システムであって、

第1暗号化キーを使用して前記第1乱数又は他のプレーヤ選択データを暗号化する前記プレーヤ端末におけるエンコーダと、

前記第1暗号化キーに対応する少なくとも1つの復号キーを記憶する前記ゲーム・サーバにおけるデータベースと、

前記少なくとも1つの復号キーを使用して前記第1乱数又は前記他のプレーヤ選択データを復号する前記ゲーム・サーバにおける復号器とを更に包含する電子ゲーム・システム。

14. 請求項3記載の電子ゲーム・システムであって、

秘密暗号化キーを使用して前記第1乱数又は他のプレーヤ選択データを暗号化する前記プレーヤ端末における暗号化器と、

公開復号キーを使用して前記第1乱数又は前記他のプレーヤ選択データを復号する前記ゲーム・サーバにおける復号器とを更に包含する電子ゲーム・システム。

15. 電子ゲーム・システム用ゲーム・サーバであって、

第1乱数を発生するプロセッサと、

別個装置において発生された第2乱数を受信する受信機と、

前記第1乱数と前記第2乱数とに基づいてゲーム結果を発生するプロセッサと

、

前記第1乱数と前記第2乱数とが独立に発生されることを保証するプロセッサと

を含むゲーム・サーバ。

16. 電子ゲーム・システム用プレーヤ端末であって、

第1乱数を発生するプロセッサと、

別個装置へ前記第1乱数を送信する送信機と、

前記第1乱数と前記別個装置で発生された前記第2乱数とに基づくゲーム結果を受信する受信機と、

前記第1乱数と前記第2乱数とが独立に発生されることを保証するプロセッサと

を含むプレーヤ端末。

17. 第1電子システムと第2電子システムとを含むシステム内でプレーさ

れる電子ゲームを制御する方法であって、

前記第1電子システムにおいて第1乱数を発生するステップと、

第2電子システムにおいて第2乱数を発生するステップと、

前記第1電子システムと前記第2電子システムとの間で前記第1乱数と前記第2乱数とを交換するステップと、

前記第1乱数と前記第2乱数とが独立に発生されることを保証するステップとを含む方法。

18. ゲーム・サーバと1つ以上のプレーヤ端末とを含むシステム内でプレーされる電子ゲームを制御する方法であって、

前記ゲーム・サーバにおいて第1乱数を発生するステップと、

前記プレーヤ端末において第2乱数を発生するステップと、

前記ゲーム・サーバにおいて前記第1乱数をコード化するステップと、

前記プレーヤ端末において前記第2乱数をコード化するステップと、

前記プレーヤ端末から前記ゲーム・サーバへプレーヤによってコード化された数を送信するステップと、

前記プレーヤ端末から前記ゲーム・サーバへプレーヤ・デコーディング・キーを送信するステップと、

前記第2乱数を得るために前記ゲーム・サーバにおいて前記プレーヤによってコード化された数をデコードするステップと

を含む方法。

19. ゲーム・サーバとプレーヤ端末とを含むゲーム・システム用ゲーム・

サーバにおいて、

第1乱数を発生するステップと、

前記第1乱数をコード化するステップと、

前記プレーヤ端末からプレーヤによってコード化された数を受信するステップと、

前記プレーヤ端末からプレーヤ・デコーディング・キーを受信するステップと、

前記プレーヤ端末へサーバ・デコーディング・キーを送信するステップと、

第2乱数を得るために前記プレーヤによってコード化された数をデコードする

ステップと

を含む方法。

20. 請求項19記載の電子ゲームを制御する方法であって、

前記プレーヤ端末へサーバによってコード化された数を送信するステップ

を更に含む方法。

21. ゲーム・サーバとプレーヤ端末とを含むゲーム・システム用プレーヤ端末において、

第1乱数を発生するステップと、

前記第1乱数をコード化するステップと、

前記ゲーム・サーバへ前記コード化された第1乱数を送信するステップと、

前記ゲーム・サーバへプレーヤ・デコーディング・キーを送信するステップと、

前記第1乱数と前記ゲーム・サーバにおいて発生された第2乱数とに基づくゲーム結果を受信するステップと

を含む方法。

22. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境用ゲーム・サーバにおいて、電子ゲームを制御する方法であって、

第1乱数を発生するステップと、

前記第1乱数を記憶するステップと、

前記プレーヤ端末からコード化された第2乱数を受信するステップと、  
前記プレーヤ端末からデコーディング・キーを受信するステップと、  
前記デコーディング・キーを使用して前記コード化された第2乱数をデコードするステップと  
を含む方法。

23. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境のプレーヤ端末において、電子ゲームを制御する方法であって、

第1乱数を発生するステップと、  
前記第1乱数をコード化するステップと、  
前記ゲーム・サーバへ前記コード化された第1乱数を送信するステップと、  
前記ゲーム・サーバが第2乱数を発生した後前記ゲーム・サーバへデコーディング・キーを送信するステップと、  
前記ゲーム・サーバから前記第1乱数と前記第2乱数とに基づくゲーム結果を受信するステップと  
を含む方法。

24. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境用ゲーム・サーバにおいて、電子ゲームを制御する方法であって、

第1乱数を発生するステップと、  
前記第1乱数をコード化するステップと、  
前記プレーヤ端末へ前記コード化された第1乱数を送信するステップと、  
前記プレーヤ端末から第2乱数を受信するステップと、  
前記プレーヤ端末から前記乱数が受信された後又は受信されるのと実質的に同時に前記プレーヤ端末へデコーディング・キーを送信するステップと  
を含む方法。

25. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境用プレーヤ端末において、ゲーム結果を得る方法であって、

前記ゲーム・サーバからコード化された第1乱数を受信するステップと、  
第2乱数を発生するステップと、

前記ゲーム・サーバへ前記第2乱数を送信するステップと、  
前記ゲーム・サーバへ前記第2乱数を送信した後又は送信するのと実質的に同時に前記ゲーム・サーバからデコーディング・キーを受信するステップと、  
前記ゲーム・サーバから前記第1乱数と前記第2乱数とに基づくゲーム結果を受信するステップと  
を含む方法。

26. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境用ゲーム・サーバにおいて、電子ゲームを制御する方法であって、  
第1乱数を発生するステップと、  
前記プレーヤ端末から第2乱数を受信するステップと、  
前記プレーヤ端末から前記第2乱数が受信されるのと実質的に同時に前記プレーヤ端末へ前記第1乱数を送信するステップと  
を含む方法。

27. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境用プレーヤ端末において、ゲーム結果を得る方法であって、  
第1乱数を発生するステップと、  
前記ゲーム・サーバから第2乱数を受信するステップと、  
前記ゲーム・サーバから前記第2乱数が受信されるのと実質的に同時に前記ゲーム・サーバへ前記第1乱数を送信するステップと、  
前記ゲーム・サーバからゲーム結果を受信するステップであって、前記ゲーム結果が前記第1乱数と前記第2乱数とに基づいている前記ゲーム結果を受信するステップと  
を含む方法。

28. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境用ゲーム・サーバにおいて、電子ゲームを制御する方法であって、  
第1乱数を発生するステップと、  
前記第1乱数を記憶するステップと、  
前記プレーヤ端末からコード化された第2乱数を受信するステップと、

データベースからプレーヤ・コード化キーを検索するステップと、  
前記プレーヤ・コード化キーを使用して前記コード化された第2乱数をデコードするステップと  
を含む方法。

29. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境のプレーヤ端末において、ゲーム結果を得る方法であって、

第1乱数を発生するステップと、  
指定プレーヤ・コード化キーを使用して前記第1乱数をコード化するステップと、  
前記ゲーム・サーバへ記コード化された第1乱数を送信するステップと、  
前記ゲーム・サーバから前記第1乱数に基づくゲーム結果を受信するステップと  
を含む方法。

30. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境用ゲーム・サーバにおいて、電子ゲームを制御する方法であって、

第1乱数を発生するステップと、  
前記第1乱数を記憶するステップと、  
前記プレーヤ端末からコード化された第2乱数を受信するステップと、  
データベースから公開プレーヤ・コード化キーを検索するステップと、  
前記公開プレーヤ・コード化キーを使用して前記コード化された第2乱数をデコードするステップと  
を含む方法。

31. ゲーム・サーバとプレーヤ端末とを有する電子ゲーム環境のプレーヤ端末において、ゲーム結果を得る方法であって、

第1乱数を発生するステップと、  
秘密プレーヤ・コード化キーを使用して前記第1乱数をコード化するステップと、  
前記ゲーム・サーバへ前記コード化された第1乱数を送信するステップと、

前記ゲーム・サーバから前記第1乱数と前記第2乱数とに基づくゲーム結果を受信するステップとを含む方法。

## 【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US97/23977

<b>A. CLASSIFICATION OF SUBJECT MATTER</b> IPC(6) : A63F 9/24 US CL : 463/22, 29 According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) U.S. : 463/10-13, 16-17, 22, 25, 29; 364/412; 380/10, 21 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X — Y	US 5,269,521 A (ROSSIDES) 14 December 1993, column 31, lines 15-55.	1-6, 8-10, 13-26, 28-32, and 47-52
Y, P	US 5,643,086 A (ALCORN et al) 01 July 1997, see col. 1, lines 38-60.	11, 12, 45, and 46
X	US 5,557,518 A (ROSEN) 17 September 1996, col. 19, lines 40-61.	1 and 17
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* "A"	Special categories of cited documents: document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"B"	earlier document published on or after the international filing date	"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, each combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other events	"A" document member of the same patent family
"P"	document published prior to the international filing date but later than the priority date claimed	
Date of the actual completion of the international search 23 JUNE 1998		Date of mailing of the international search report 20 JUL 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230		Authorized officer JAMES SCHAAF Paralegal Specialist Group 3000 3700 Telephone No. (703) 308-1140

Form PCT/ISA/210 (second sheet)(July 1992)\*

---

フロントページの続き

(81)指定国 EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW

(72)発明者 ジョラシュ, ジェームス, エイ.  
アメリカ合衆国, コネチカット, スタンフ  
ォード, フォレスト ストリート 25, ア  
パートメント 5ジー

